UNIVERSITY OF TAMPERE
School of Management

HUMAN ELEMENT OF CORPORATE ESPIONAGE RISK MANAGEMENT – LITERATURE REVIEW ON ASSESSMENT AND CONTROL OF OUTSIDER AND INSIDER THREATS

Insurance Science
Master's Thesis
April 2015
Author: Jarkko Sandberg

Supervisor: Olli-Pekka Ruuskanen

ABSTRACT

University of Tampere	School of Management, Insurance Science
Author:	SANDBERG JARKKO
Title:	Human Element of Corporate Espionage Risk Management – Literature Review on Assessment and Control of Outsider and Insider Threats
Master's Thesis:	78 pages
Date:	April 2015
Keywords:	Corporate Espionage, Information Risk Management, Insider Threat, Social Engineering, Advanced Persistent Threat

The primary purpose of this study is to determine how suitable human risk management controls are against corporate espionage. Information risks are ascending problem with corporations all over the world. Cyber attacks are commonplace, and the attackers are often trying to compromise valuable data assets. These malicious targeted attacks are bypassing traditional information security controls; therefore, organizations are endangered by these threats. Since the traditional information security measures cannot effectively prevent trade secret thefts, companies must look for alternative remedies to mitigate the risks of corporate espionage. One eligible solution is to focus on the human element of information risks management, and thereby defeating the malicious corporate spies.

This theoretical thesis aims to consolidate various sources of research literature in order to approach targeted threats from a human risk management perspective. The literature review incorporates research from various fields, such as cyber security, information risk management, corporate espionage, insider threat, and social engineering. The objective of the thesis is to merge these fields together, and identify the most suitable risk management controls against corporate espionage activities. Corporate espionage activities often include exfiltrating valuable data via Internet and information technology. Hence, the espionage activities are occurring in a challenging risk environment, which is introduced in this thesis.

A large part of this thesis focuses on the assessment of insider and outsider threats. These threat actors are analyzed and evaluated thoroughly, focusing on the motivation and opportunity of the perpetrators. The two main attack methods are social engineering and malicious insider activity. These attack methods are extremely dangerous to companies of all size, and risk management literature has largely ignored the subject. The legal ramifications to the problems are inadequate as well, since corporate espionage attacks often emanate from states with weaker legislation towards Internet crimes. However, companies can brace themselves against malicious insider activity and social engineering with careful assessment and risk management decisions. The research literature supports the view that the most effective ways to mitigate risks of corporate espionage is to control the awareness and behavior of organization's employees. The corporate espionage risks will not subside by themselves; hence, organizations must reinforce their policies and data management procedures.

Table of Contents

1 INTRODUCTION

1.1 Background & Prior Research

Cyber security and information risk management have been extremely topical subjects recently because of the large-scale cyber attacks are targeting organizations all around the world. In addition, information security has become a matter of national security. Especially in the United States, large corporations have been publicly targets of data breaches and other cyber attacks. During 2014, U.S corporations suffered total of 293 breaches that were made public, of which 145 were caused by hacking or malware (privacyrights.org). However, the real number is significantly larger, since majority of the occurrences will go unreported. Companies are reluctant to report breaches for many reasons, and underreporting is extremely common. (Moore, 2010) The biggest reason is the bad publicity, since publicly disclosed IT security breaches have reduced the company's stock prices in the short term (Bandyopadhyay et all, 2009, 69). In addition, companies are worried that their clients, employees, and shareholders will interpret the breaches as weaknesses, and that they might abandon the compromised company. (Moore, 2010)

Cyber criminals are leveraging malware, bots, and other attack forms to attack organizations for financial or political agendas. Cybercrime has become a well-structured and organized criminal activity, and the actors have the intelligence, time, and resources to execute long-lasting attacks to reach their goals. The complexity of the risks is endangering companies all around the world, since cyber risk mitigation methods are lagging behind the attackers' ingenuity. (Ponemon Institute, 2012)

Bypassing traditional security controls, such as firewalls and anti-virus software, require excellent hacking skills from the attackers. Organizations' security professionals have failed to understand that cyber criminals–as well as corporate spies–are following the path of least resistance. Perpetrators look for the weakest part of the organization's defense. Therefore, a substantial part of the cyber attacks are designed to target the endpoint of the computer, which is generally the human who is using it. (Rogers, 2007)

The business world today is constantly moving towards more technology orientated, and this development has brought completely new risks and a new risk environment. Approaching the issue in criminal perspective, it is safe to say that human behavior has not changed in the course of cyber development, since crimes are committed on the same grounds but with different methods. Bank robberies have become stealthy hacker attacks, and terrorists can cause damage remotely through Internet, far away from the target. The information has become so crucial part of a company that the substantial value of a company lies in the information it retains. Without the given information, there might be no competitive advantage over competitors. Therefore, corporate espionage is perhaps the most devastating risk to certain companies that possess unique technology or other trade secrets. According to a survey made by Internet security company Kaspersky Lab (2013), a significant proportion of security incidents resulting in a loss of valuable data were internal. Internal incidents were caused intentionally or negligently by employees' actions, and 85% of the surveyed companies reported insider incidents.

Most of the information risk management procedures are traditionally channeled to IT department and anti-virus software companies that develop technical solutions, such as firewalls and intrusion detection systems. Although all companies invest in these solutions, security breaches occur, since attackers have evolved to circumvent technical and process-based security controls. One of the main reasons for this is the human element of information security. There are technical, physical, and human elements in information security, and the technology and processes are only as competent as the humans that use them. Most of the targeted cyber attacks are compromising a human, not the computer or system; therefore, exploiting human vulnerabilities has become common attack vector. (Dontamsetti & Narayanan, 2008)

Information security is apparently more than just technical solutions and IT staff's problem. There are myriad of prior research about information risk management, but most of these studies approach the issue with technical measures. There are also studies that evaluate insurance solutions to cover information risks and cyber attacks. However the insurance solutions do not mitigate the risk of trade secret thefts. (Bandyopahhyay et all, 2009)

Focusing on the recent data breaches and specific incidents, cyber attacks can be used for effective corporate espionage attacks against companies. However, these attacks rely mostly on social engineering rather than complicated malware. (Thonnard et all, 2012) Corporate espio-

nage is a serious threat to companies, since the intellectual property and proprietary information they posses, are usually the most valuable assets of the organization. Companies suffer great financial losses due to trade secret thefts and espionage attacks. (O'Hara, 2010) However, there is no adequate research about corporate espionage risk management. Given the seriousness of the risk, it is important to approach trade secret theft related issues from risk management perspective, and to understand the mitigation process of these risks to corporations all around the world. According to Moore (2010), the combination of secrecy, fear, uncertainty, and doubt is complicating the corporate espionage related information security.

1.2 Research Objectives & Scope of the Research

This thesis focuses on the risk assessment of corporate espionage in the information risk environment. The focus is on the human element of outsider and insider threats. As mentioned in the preceding chapter, there are two different inadequacies in the information risk management field. Firstly, information risk management is still considered way too technology orientated, and the trade secret thefts are largely ignored in the information risk studies. Secondly, the lack of corporate espionage risk management research is a severe problem. Hence, the objective of this study is to link together these two topics, and to approach the issue from the operational risk management perspective.

The first research problems is:

- Which non-technical risk management controls are most suitable against insider and outsider threats?

This research problem aims to encourage risk management perspective towards the corporate espionage risks. The risk focus will be on the social engineering and the behavior of malicious insiders.

The second research problem is:

- How information risk management procedures should take corporate espionage threats into consideration?

This research problem aims to introduce the challenges of the new technological risk environment where the corporate espionage occurs, and how these risks should be approached.

The goal of these research problems is to provide new research data, and to enrich the existing literature theory. The first objective is to unite two different concepts through intensive harvesting of literature. These two concepts are information risk and corporate espionage. Information risks and corporate espionage are occurring in information risk environment (Cole, 2012 ; Nasheri, 2001), and this is why the main focus of the second chapter is to merge corporate espionage risks to the concept of information risk. Another main objective of the study is to bring up challenges of human information risk management processes, regarding to outsider and insider threats. In addition, this study is making a comparison of the outsider and insider threats.

The information risk management is a broad topic. Therefore, many information risks are left out from this research. The scope of the research involves human risk management solutions against human elements of the insider and outsider threats. This somewhat narrow perspective is necessary, since there are large amount of literature concerning human information risk management with technical measures. Physical risk management solutions, such as physical data isolation, are also left out from this study; while they are effective risk management solutions, they also complicate the legitimate users to perform their job (Cole, 2012, 265).

Corporate espionage risks are more commonplace in the United States than in other countries on the grounds that the U.S. possesses the largest abundance of commercial innovations. In other words, the U.S. corporations are more attractive targets for spying activity, because they simply have more to steal from. Therefore, the U.S. federal legislation towards corporate espionage is the most advanced in the world, and Europe has substantially weaker laws against trade secret theft (businessinsider.com). For this reason, the legislative parts of this thesis are written mostly from the U.S. point of view. However, I will address some legislative issues also from the Finnish point of view. Since the matters of corporate espionage and cyber attacks are addressed the most in the United States, the research literature of this thesis is mostly American. However, espionage and cyber attacks are occurring in Europe and in Finland as well; therefore, subjects introduced in this thesis applies to any other country as well.

1.3 Methodology

Since the method is literature review, this study tries to provide relevant and novel information from various areas of literature. These areas of literature can be divided in three categories, which are:

- Information risk management; including cyber security, cyber threats, advanced persistent threats, and insider threats.
- Trade secret thefts; including corporate espionage, economic espionage, industrial espionage, cyber espionage, and electronic espionage.
- Risk management literature, emphasizing Enterprise Risk Management (ERM) and operational risk management.

This research is qualitative by definition, and it is a descriptive literature review. The purpose of the literature review is to identify, assess, and consolidate published research data. This is done by examining published studies and literature, and approaching the research problems with a relatively theoretical vantage point. As in the word "review", the re -prefix refers to rewriting and reassessing, which is done critically and with a new perspective. (Salminen, 2011)

According to Baumeister & Leary (1997), there are three main reasons for literature review as a research method; a qualitative literature review is able to (1) develop, (2) evaluate, and (3) consolidate existing theories (Salminen, 2011). The objective of this thesis is to consolidate existing literature and research from different fields, and the precise research method is narrative literature review. Narrative method is the most adequate when the research problems are broad (Salminen, 2011, 6). Given the broadness of the research problems of this thesis, the method of choice is narrative and descriptive research literature review. Although the method is narrative, there are some elements of integrative literature review as well. The integrative literature review has a critical approach to the research material (Salminen, 2011).

The method of this thesis was chosen mostly because of the delicacy of the subject. In addition, the existing literature about information security management and cyber security are

subjects that are not studied enough in proportion of their importance; hence, the existing research was in need of consolidation and update.

1.4 Structure & Framework of the Research

This research consists of five main chapters. The first chapter is introduction to the research, where the objective, background, and the framework of the research are outlined. Some key definitions will also be opened up in chapter one.

The second part of the study is about the risk environment where the trade secret thefts and cyber espionage transpire. Cyber environment as well as information risk concept will be introduced before going to the characteristics and peculiarities of corporate espionage and trade secrets. In the beginning of the corporate espionage chapter, the definition of trade secrets will be introduced. Consequently, the definition of corporate espionage will be outlined, as well as the brief history and development of espionage actors, targets, and motivation. Finally, the legal issues relating to prosecution and international law will be introduced.

Third part consists of two different attack methods regarding to corporate espionage and trade secret thefts; external threats done by outsiders, and insider threats. The main attack vector of outsider threats, such as APTs, is the social engineering. In addition, the threats of malicious insiders will be presented in chapter three. The main focus of this part of the thesis is the perception and assessment of corporate espionage related risks. Since the scope of the thesis is human element of information risk management, I will obviously focus on the non-technical parts of trade secret thefts, particularly social engineering done by outsiders, and malicious activity done by insiders. The insiders are mostly employees but also contracted consultants and on-site workers.

The fourth part of the thesis will consider the risk management processes, and especially those processes that can help to control and assess the risks introduced in the second part of the thesis. The focus of this literature research is on the human risk management controls. In the fourth chapter, the most convenient risk management controls will be introduced. The objective is to analyze the risk management controls, especially their suitability to insider and

outsider threats. The final chapter will conclude this thesis, and I will critically evaluate the risks and risk controls, as well as the risk environment introduced in the second chapter.

The theoretical framework is illustrated in the figure 1 below. From the framework figure, it is easy to notice that this thesis has two distinct parts: risk environment, and risk management controls. Corporate espionage, information risk, outsider threat, and outsider threat form the risk environment. These topics are reviewed in the second and the third chapter of this thesis. The fourth chapter will address the risks management controls that are–answering to the main research question–most suitable against insider and outsider threats.

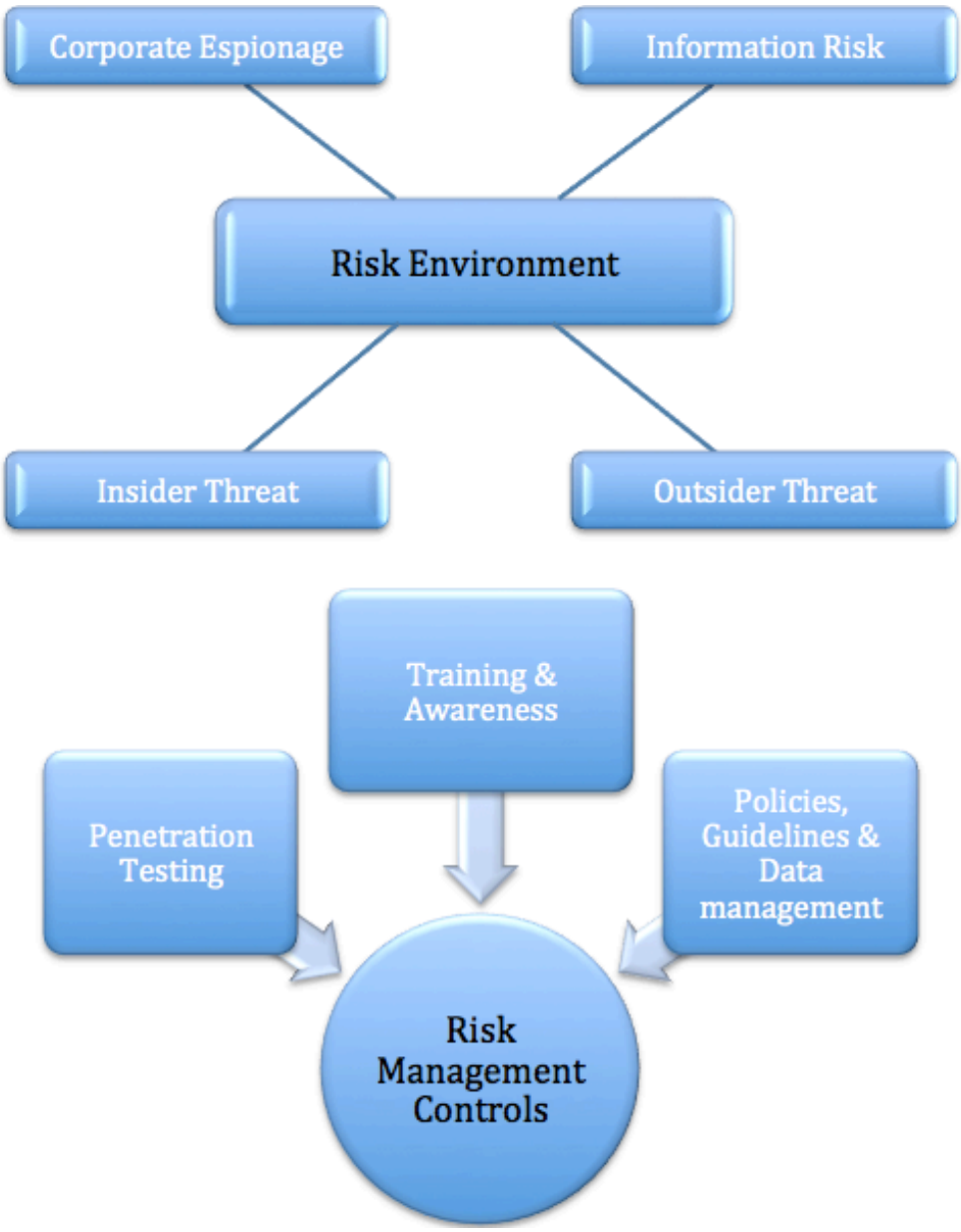

Figure 1. Theoretical Framework of the Research

1.5 Key Definitions

Threat is the potential for an event that would damage or compromise an asset, such as trade secret theft.

Risk is a combination of a *threat*, probability, and impact.

Information risk is considered a synonym for *cyber risk* in this thesis.

Attack Vector is a path or means by which a hacker can gain access to computer. Attack vectors enable attackers to exploit system vulnerabilities, including the human element. (searchsecurity.techtarget.com)

Corporate espionage is an activity where someone is illegally stealing, copying or sabotaging an organization's confidential or secret information that has independent economic value. This information is considered a *trade secret*, if it is kept in secrecy with reasonable efforts. (Fink, 2002)

Cyber attack is an attack on cyber resources. The attack is typically carried out by cyber means. (Bodeau et all, 2011, 7)

Malware is malicious software, which is a prepackaged exploitation of vulnerability (Finney, 2014)

Vulnerability is a flaw or weakness in the asset's defense that could be exploited by a threat (Peltier, 2013, 53). According to National Institute of Standards and Technology SP 800-80, defines vulnerability "a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy."

2 CORPORATE ESPIONAGE AS AN INFORMATION RISK

Corporate espionage has become a huge threat to companies in the developed world, and formulas, patents, business expansion plans, customer lists, pricing information, product launch information, and other valuable trade secrets are endangered. Espionage has become more deceptive because of the interconnectivity of people within the business environment. People change workplaces more often, and people stay connected to each other via social media; therefore, malicious companies have more opportunities to recruit insiders. Espionage is also facilitated by the new information age. Malicious companies can deploy malware to bypass organizations' defense, or obtain credentials with targeted hacking activities. (Burges & Powers, 2011 ; Fink, 2002)

2.1 Cyber Environment

Security is a basic need for every person, as well as for every corporation and state. Issues and deficiencies relating to cyber security are usually thought to be technical or technology related. However, a substantial part of the cyber security is made by strategical and managerial decisions. According to Limnéll, Majewski, and Salminen (2014, 47), only one-third of the cyber security is technology-orientated. Traditionally in the corporations, cyber security is understood mainly by its technological methods, for instance trying to implement adequate firewall and antivirus software.

2.1.1 Cyber Security

In most of the corporations, a separate IT- department is accountable for the whole concept of cyber security. Sometimes the department that is in charge of cyber security is outsourced to a third party. With a separate department or a third party dealing with security issues, it is difficult to ensure that the cyber security is aligned with organization's risk management department and other operations. Cyber security should be linked with all the functions of the corporation; hence, the question of cyber security should be raised to a corporate level strategic matter. To be more precise, from the modern business standpoint, cyber security should be

considered throughout the entire process, including designing, development and assembling the organization's operations. The cyber security is optimal when it is established inside the systems, programs and solutions. However, the common flaw of cyber security is that the security part is established afterwards. (Limnéll et all, 2014) Organizations and people in general are extending the usability and connectivity of networks, without paying attention to the risks involved. This behavior is increasing incidents in the cyber environment, and hinders the mitigation process of cyber risks. (Gregory, 2003)

Computing and computing systems have largely changed the modern business environment from what it was few decades ago. The society where we live in today is dependent on the functioning of networked computer systems that are mostly automated. These systems appear in almost every sector of economy, however some industries are more advanced in technological transformation. The core advance of digitalization and information age was to facilitate human interactions, and to enhance the possibilities of distribution and transportation of information. However, the agile flow of information has caused significant problems for the protection of intellectual property laws and corporate espionage. (Nasheri, 2005, 31-32)

Cyber security went through its first development circle in the mid 1990s, when organizations realized the necessity of protecting the integrity of their security systems as they were connecting operating systems to the Internet. Before that era, only internal networks connected different parts of the organization. At early developing stages, security professionals met with resistance, since the information security was criticized as a non-productive activity that drains organization's resources and reduces the pace of innovation. Therefore, security professionals' opinions were blatantly ignored. However, when years went by, chief executive officers and shareholders started to acknowledge the danger of a bad information security. The large-scale virus attacks, such as Melissa (year 1999) and ILoveYou (year 2000) were to be the starting point of the awareness of cyber security issues. When these attacks spread around the world making damage, some executives started to listen security professionals more closely. (Gregory, 2003)

In the cyber environment, there is a constant race where two rival sides are competing against each other. States, corporations, armies, and Internet security companies constantly seek to improve the defense mechanisms of their operating systems and services. On the other side, cyber criminals, hackers, terrorists, and malicious state actors are trying to find vulnerabilities

to exploit. The malicious actors are trying to attack against corporations and state entities worldwide, with increasingly sophisticated measures. (Limnéll et all, 2014) The attitude towards cyber security can be seen as a problem and a risk to organization's security. In addition, many individuals consider cyber security as a tax, since organizations do not receive any tangible benefit from cyber security. The whole information security is seen as a mere obligatory expense. (Gregory, 2003, 3)

Cyber security is problematic environment, since operating systems, as well as software and hardware, have tremendously fast development cycles. This also applies to attack measures and malware. Since the cyber environment changes, so do the risks involved. Once the investment on cyber security has been made, it is essential to update them constantly. Unpatched security software is not able to detect new threats, and possibly not even able to counter them. (Biener et all, 2015)

The anonymity and ease of use of Internet makes it the most convenient measure for criminals to steal sensitive business data. A simple cyber threat or corporate espionage attack might cause damage worth hundreds of millions. And this might be the case, even though the hacker does not reveal the stolen or copied information to anyone, since some hackers are stealing the valuable economic information only for the sake of challenge. These people commit hacker attacks for various reasons, and they are not motivated by financial gains. An example of non-economic attack is the ascending phenomenon of hactivism, where hacker groups are targeting organizations to make a point or trying to stop organizations from doing something. These attacks try to cause reputational damage or embarrassment. When the company puts up a more sophisticated firewall or intrusion detection system, hactivists might just rejoice due to the new demanding barrier of intrusion. However, when these attacks get through the organization's network, the damage is already done. One attack that compromises the security causes the organization to redesign their systems, and this is costly. Redesigning is essential, since the entire organization is now proved to lack security, and the organization's defense is open for other attacks as well. Hackers, who are committing these attacks as a prank, do not realize the damage they are doing, since even a little amount of downtime for the organization's network is a serious threat to its operations. (Cole, 2012 ; Fink, 2002)

2.1.2 Laws of Cyber World

Cyber world is an extremely dynamic environment and it is not bound by physical laws. Cyberspace is constantly moving, and it has a high degree of complexity. Nowadays, cyberspace is accepted as a domain equal to land, air, sea, and space. In order to better understand the cyber environment and its peculiarities, certain principles must be presented. According to Limnéll et all (2014), there are five fundamentals regarding to the laws of cyber environment. These are time, space, anonymity, asymmetry, and efficiency.

Time is very relative conception in cyber world. In a sense, time loses its meaning in cyber word. Because of the Internet, malicious attackers can execute their attacks from anywhere around the world, without any time delay. Of course, the planning of the attack takes time, but the actual delivery of the attack is not bound by physical limits of time. The second fundamental is *space*. Cyber world is neither bound by geographical distance, since almost everything is connected through Internet. Third concept is *anonymity*. Being anonymous in the Internet is a rather easy task. It is difficult to identify the attacker or hacker, and trace back the inception of the attack. If you are able to cover your tracks, there is no fear of being caught. The IP address of the attacker might be possible to track down, but it is impossible to say who is really using the address. In the anonymous cyber world, a same person can also use many different identities. (Limnél et all, 2014)

The fourth concept of cyber world is *asymmetry*. Cyber environment enables small actors to achieve large damage and serious harm against big players, such as global corporations or government entities. Hackers, criminals and terrorists can act all alone or in small groups, yet they can harass numerous different targets at the same time or put vast organizations on their knees. In cyber world, the attacker has a substantial advantage over the defender. Conducting a cyber-attack does not consume the attacker's resources, therefore attacks can be done persistently, and failures do not stop attackers from trying. The last law of cyber world is *efficiency*, which is analogous to asymmetry of cyber world. In cyber environment, it is possible to perform many activities at the same time. A successful attack can infiltrate the network, compromise information, interfere connections, and sabotage critical infrastructure. The attack can manage to complete all these actions at the same time. The attacker's ability to accomplish many different activities at the same time, is a fundamental quality of cyber environ-

ment. (Limnél et all, 2014) These qualities make information risks unique and difficult to comprehend.

2.2 Information Risks

Information risks are crucial to understand, if an organization wants to survive in the new landscape of cyber threats. The objective of information risk management is to manage three basic attributes of information; confidentiality, integrity, and availability. Availability deals with the problems that information resources and data should always be available to the owner of the information, whereas integrity concerns the inviolability of information resources. Regarding to trade secret thefts and corporate espionage, confidentiality can be considered the most important attribute of information risk. Malicious insiders or external targeted threats are prone to offend the confidentiality of information assets. (Alexander, 2008) Biener et all (2015), defines cyber risks as "operational risks to information and technology assets that have consequences affecting the confidentiality, availability or integrity of information or information systems".

Cyber risks derive from many different sources, from organization's operations and outside the organization. Basel III and Solvency II regulation frameworks categorize the sources of cyber risks in four different areas: (1) actions of people, (2) systems and technology failures, (3) failed internal processes, and (4) external events. The categories number 2 and 3 are technical by their nature. Category number 4 includes external risks, such as natural and human catastrophes, regulatory compliance risks, market condition failures, and service dependencies. However, category number 1, actions of people, is where the trade secret threats derive from. The actions of people category is divided to three different subcategories:

1. Inadvertent action, which is an unintentional action without malicious intent, such as error, omission and mistake.
2. Deliberate action towards organization's possession, such as fraud, theft, and sabotage.
3. Inaction, where employees fail to act due to their lack of skills or guidance.

(Biener et all, 2015, 4)

Inadvertent actions constitute a large proportion of occurred information risks. Employees commit errors and omissions while they are working in haste. The number of error-based risks is larger than deliberate actions, but malicious theft and fraud are extremely injurious to organizations. (Ponemon Institute, 2012)

The legislation related problems are also encumbering the risk environment. The legislators of European Union have drawn up several information security related directives, which have been implemented to all member states. However, in European countries, such as in Finland, there is not a separate law that would govern information security. Hence, there are acts, such as the Act on the Protection of Privacy in Electronic Communication (2004) and the Information Society Code (2014) that contain norms about information security. The largest obstacle in enacting a separate law is the fast development cycles of computer technology. (Laaksonen et all, 2006)

2.2.1 Threats to Information Security

The state of perfect security is impossible to attain. Threats and vulnerabilities always exist, no matter how advanced the security systems are. This applies to both physical world and cyber environment. The challenge is to adjust the level of security to a sufficient level. The level is determined by every entity on its own initiative. (Limnél et all, 2014) A threat is anyone or anything that poses danger to the information security, where the target of the threat is information, computing resources, users, or data. Threats can be divided into two categories; external and internal threats, depending on the source of the threat. (Nayak & Rao, 2014, 31)

Internal threats derive from inside the organization, such as the misconduct of employees. These threats arise from improper security policies, weak system and data administration, and the lack of security awareness. External threats derive from outside the organization, especially from the environment in which the organization operates. (Nayak & Rao, 2014, 31-33) I will not dwell any deeper to these threats in this part of the thesis. To demonstrate the abundance of the threats to information security, the most important external threats are portrayed in the figure 2.

Figure 2. External Threats to Information Security (Nayak & Rao, 2014)

As we can observe in the figure 2, the range of threats to information security is diverse. Because of the large variety of these threats, information risks are difficult to understand completely and to manage efficiently.

Cyber threats can be divided into two categories by the vulnerabilities they exploit; syntactic or semantic. Syntactic attacks exploit technical vulnerabilities, whereas semantic attacks exploit social vulnerabilities. However, many attacks have characteristics of both semantic and syntactic attack types. These blended attacks use technical tools to facilitate social engineering in trade secret threats. (Choo, 2011)

2.2.2 Information Security Vulnerabilities

Vulnerabilities are usually seen as unintentional failures that incur inside the network. However, vulnerabilities can be consequences of a deliberate act. Vulnerabilities are weaknesses that an attacker may exploit. In information security environment, these weaknesses are associated with security procedures, technical controls, physical controls or other controls of as-

sets. Typically vulnerabilities are known as a technical issue, but humans as well cause significant part of the vulnerabilities, especially in the case of information confidentiality. Poor user account management is an example of important non-technical vulnerability, although it has technical attributes as well. (Gregory, 2003 ; Jerman-Blažič, 2008) Sometimes human actions cause technical vulnerabilities. Software engineers are on a constant hurry to develop their programs to better serve their customers and launch programs before competitors. Therefore, the necessary amount of testing is many times left out from the developing process. This misstep sometimes leaves substantial defects to the programs. (Cole, 2001)

One major source of vulnerabilities is software defects, also known as bugs. They usually cause abnormal functionality in software. An example of software bug is a buffer overrun, where a program accepts input without checking the size of it. The amount of data might be larger than the storage of the program has prepared for it. Therefore, the exceeding data will overwrite some other program storage, and the data can include malicious code. A large amount of hacker attacks exploit buffer overruns. This vulnerability for example, is usually a deliberate act of a malicious attacker. There are of course unintentional technical vulnerabilities as well, such as calculation errors. Software coding is largely about mathematics and calculations; hence the risk of error always exists. Programmers also sometimes fail to test the boundary conditions of the application. An example of this was the Y2K problem with two-digit years 99 and 00. The main problem in software security, and overall information security as well, is the huge cost of adding superb security in products and people. In contrast, the cost of completely ignoring security is small. Therefore, the incentives to strengthen the level of information security diminish, while the expenses are high and the benefits are hard to measure. (Gregory, 2003, 19-20 ; Jerman-Blažič, 2008)

The organization's connectivity to outer networks also predisposes the organization to vulnerabilities. Typically, an organization has a large amount of entry points, and each of those can be a path for a malicious intruder. A large organization has to efficiently manage its Internet connections. An organization might have back-door connections to Internet, which is used by test labs or remote access purposes. These other connections might not have the same extent of protection as the main Internet connection, thus they should be considered "outside" networks. (Limnél et all, 2014) Technical vulnerabilities are a cumbersome issue to the organization's risk environment, since social engineers and malicious insiders can deploy the weaknesses in the technical perimeter, together with human vulnerabilities.

2.3 Corporate Espionage

The basics of the threat of corporate espionage have not changed significantly in the era of information technology. However, the Internet and information age have re-tooled some espionage techniques. The foundation of the threat is still the same, but the technology has disguised the threat to be broader and faster, as well as more subtle and deceptive. Technology has changed some of the attack vectors and some features of the attacks. Nevertheless, the technology does not attack by itself, since the root of all espionage is always a human, whether it is an insider or outsider. Malicious economic spies are usually motivated by financial greed, and their attacks include deception and hidden actions. (Burgess & Power, 2006 ; Skinner, 2013)

Corporate espionage is a serious risk to companies worldwide, and all it takes is one single person or a competitor to endanger a company. The person can be found either inside or outside the company. A common misbelief is that only large corporations are prone to be targets to corporate espionage, yet many smaller organizations face the risk as well. Smaller businesses usually have more competitors than large corporations; therefore, they can be even more exposed to corporate espionage. (Fink, 2002)

To better illustrate the grave problem of corporate espionage, the figures will speak for themselves. According to The International Chamber of Commerce, the estimated fiscal loss from corporate espionage was more than $600 billion a year, and according to U.S. Commerce Department, the amount was $250 billion annually, and costing around 750 000 jobs in the United States only (Burges & Power, 2008). Due to espionage attacks, corporations all over the world are loosing incentives to develop scientific and technological innovations, and this is affecting to the nation's competitive advantage. Trade secret thefts are political issue as well. In the U.S., the gravity of the problem is already affecting the political relations with China, since China is a common culprit in espionage activity towards U.S industrial technology and government's information. (Skinner, 2013, 1168-1169)

Many companies are concentrating on the physical security by protecting their properties with a lot of effort. Companies are protecting the entrance to the office building, and fencing the

surroundings of a warehouse. However, more than 70% of a company's market value comes from intangible assets, such as trade secrets. (Fink, 2002)

In the following chapters, I will first outline the basis of trade secrets by defining their true nature according to Economic Espionage Act. After this, I will separate the differences between legal intelligence proceedings and illegal espionage activity. I will introduce a brief history and evolution of corporate espionage, and the last part deals with jurisdictional and prosecution aspects of trade secret thefts. I will also regard the corporate espionage related parts from the Finnish legislation.

2.3.1 Trade Secrets

To completely understand the depths of corporate espionage, companies have to be aware of some details of trade secrets. The most important quality of a trade secret is the *secrecy* of the information. The owner of a trade secret needs to take a protective approach to the information; otherwise, it is not considered a trade secret at all. The basic element of the trade secret cannot be generally known to the public, and it cannot be found in public domains. The owner of the secret shall not leak the valuable information to the public by any means, for example in a presentation given to students at a university. Besides being kept as a secret, a trade secret has to contain some element of novelty. The information regarding to the trade secret cannot be obvious to the competitors, nor can it be generally known to public. However, a trade secret can be a combination of public information and secret information, and the unique combination of information will create a legitimate trade secret. (Fink, 2002, 211-213)

According to the Economic Espionage Act from 1996, trade secret includes:

> *all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing…*

(Simon, 1998)

The organization that claims to possess the aforementioned trade secret, need to take *reasonable measures* to control the valuable information and to keep it secure. Therefore, the organization has to educate, train, and advice its employees on regular basis. Organizations should as well require non-disclosure forms and non-compete clauses, and limit the access of the employees to the trade secrets. (Simon, 1998 ; Fink, 2002) In his book (2002), Fink points out that the "open culture" work environment is not the best possible culture regarding to trade secret safety, since the victim of a trade secret theft has to be capable to indicate the occurrence of the crime in a court. In a highly open culture environment, it might be difficult to demonstrate that any security measures were adopted inside the organization. According to Simon (1998), additionally to the competent security measures, the organization has to be able to prove the independent economic value of the trade secret. Hence, the information should derive economic value, whether actual or potential.

2.3.2 Legality Issues

Somewhat confusing concept relating to trade secret thefts is the business intelligence, which is currently an ascending activity among organizations all over the world. This legal activity contains reconnaissance of publicly available information, such as court records, annual reports, governments documents, trade fairs, speeches made by executives, and sales reports. All this is considered open source information, and competitors can legally dwell into these documents. Even though the motives to practice business intelligence are similar to ones of corporate espionage, the methods are fundamentally different, since corporate espionage is about stealing trade secrets. (Coskun & Jacobs, 2003)

Business intelligence only analyzes and scrutinizes useful and legally available information. An example of legal business intelligence is gathering sensitive information in business and scientific seminars, or at international trade shows. Spies from competing companies can act as a potential customer or interested researcher in these open events to obtain valuable information. Competitors can also obtain large amounts of valuable information legally from requested proprietary documents prior to trial. (Coskun & Jacobs, 2003, 96-103 ; Winkler, 1996) Legal methods of acquiring trade secrets include the pressuring or "blackmailing" done by actors of foreign country. Some foreign countries, in order to allow foreign companies to do business in their land, are forcing the counterpart to divulge valuable intelligence. This

prerequisite of doing business might turn up expensive. Companies might also have to train and employ native workers in a field of critical technology. Sometimes the only way to enter a foreign market is to assemble a joint venture with a native company. Joint ventures provide great opportunities for the foreign company to tamper sensitive information from the counterpart. (Winkler, 1996, 1-2)

An important par of the business intelligence is reverse engineering, where a company is practicing legal espionage by scrutinizing a competitor's product. The purpose of reverse engineering is to get familiar with the processes and specification in the product's development and manufacture. The company that is practicing reverse engineering, tries to study the item precisely to obtain detailed understanding of the way it works. The aim is to create similar or even superior products by redesigning the product. (Coskun & Jacobs, 2003)

The thin line between illegal espionage activities and legal business intelligence is hard to define. As a rule of thumb, anything that can be considered stealing is strictly illegal. Stealing can happen in many subtle ways, which are sometimes hard to prove. Competitors can recruit a mole from the target company. In such a manner, the company has someone inside the victim organization, working in exchange for money or other benefits. These moles originate from inside and outside, meaning that the malicious company can recruit the insider or the insider can volunteer his or her services as a mole. Another commonly used method is eavesdropping target employees. This is extremely relative for employees who travel often, since hotel rooms can be eavesdropped or searched during the absence of the guest. Often overlooked because of its simplicity, dumpster diving is another effective way to spy companies. (Winkler, 1996 ; Nasheri, 2005) Since this thesis about two specified attack vectors; malicious insiders and outsider social engineering, I will not dwell any deeper into physical attack vectors, such as dumpster diving, breaking into company's premises, eavesdropping, theft of laptops and other computers, or technical attack vectors, such as keyloggers, back door exploitation, distributed denial of service attacks, etc.

2.3.3 History & Development of Corporate Espionage

To define the term corporate espionage, we will take a glance of the Economic Espionage Act of the United States of America, signed into law by Bill Clinton on October 11, 1996. The act

gave the U.S. Department of Justice authority to prosecute trade secret theft that took place in the U.S. and abroad, as well as over the Internet. Section 1831 of the Economic Espionage Act gives a broad definition of corporate espionage and the act provides a guideline of criminalized violations:

> *Culpability is determined with reference to section 1831 (a):*
> *(a) In general. Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly –*
> *(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret;*
> *(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret;*
> *(3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;*
> *(4) attempts to commit any offense described in any of paragraphs (1) through (3); or*
> *(5) conspires with one or more other persons to commit any offense described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy*

(Simon, 1998)

The Criminal Code of Finland (39/1889)–that was amended in 1990 with sections concerning espionage and trade secrets–describes the business espionage as following:

> *(I) A person who unlawfully obtains information regarding the business secret of another (1) by entering an area closed to unauthorised persons or accessing an information system protected against unauthorised persons, (2) by gaining possession of or copying a document or other record, or in another comparable manner, or (3) by using a special technical device, with the intention of unlawfully revealing this secret or unjustifiably utilising it shall be sentenced, unless a more severe penalty for the act is provided elsewhere in the law, for business espionage to a fine or to imprisonment for at most two years.*
> *(II) An attempt is punishable.*

Corporate espionage is many times more concealed and silent than other blue-collar crimes. The crime occurs usually in two different ways; a malicious insider misappropriates company's trade secret for financial benefit, or a company's competitor or a foreign state misappropriates the trade secrets to boost its competitiveness. The attack vectors vary a lot regarding to who the attacker is. Trade secret thefts occur in advanced manners, such as computer hacker attacks, wire interceptions, and with complex spying devices, or more simple ways, such as memorization, and photocopying. Competitors and governments are not the only source of spies, since vendors, investigators, business consultants, the press, and labor negotiators can be possible trade secret thieves as well. (Nasheri, 2005)

Espionage began in its current form during the First World War, when countries were trying to save time and resources in developing complex weapons, such as poison gas. These thefts were orchestrated by foreign states against each other. Nowadays, the usual target is an enterprise that holds economically valuable trade secrets. According to the U.S. Department of Justice, industrial espionage is an activity where a private U.S. company is attacked by foreign government or a foreign company with assistance of the foreign government. However, some countries have a long history of ties between government and private companies. Therefore it is hard to notice, whether the espionage was sponsored by a government or not. In modern economics, the line between private and public sector is blurred, since many companies are state owned or state financed, and politicians serve on company boards. It is important to remember that ally countries are "at war" against each other when it comes to business, because economic superiority has become more important than military superiority. Especially former communist countries have thought that spying activities will generate faster solutions to catch up in the technology competence with western countries. (Nasheri, 2005)

2.3.4 Actors, Targets & Motivation

As written earlier in this thesis**,** all companies, across all industries, are susceptible to corporate espionage, and sometimes smaller companies face even more risk of being spied than large corporations. However, some companies are more prone to be a target than others, and in this chapter, I will expose the characteristics of the companies, which draw more malicious attackers than others, as well as the basic motivation behind corporate espionage. I will also

introduce the characteristics of the mischievous companies that carry out corporate espionage attacks against other companies.

According to the section 5 in the Criminal Code of Finland (39/1889), trade secret violator is:

> *(I) A person who, in order to obtain financial benefit for himself or herself or another, or to injure another, unlawfully discloses the business secret of another or unlawfully utilises such a business secret, having gained knowledge of the secret (1) while in the service of another, (2) while acting as a member of the administrative board or the board of directors, the managing director, auditor or receiver of a corporation or a foundation or in comparable duties, (3) while performing a duty on behalf of another or otherwise in a fiduciary business relationship, or (4) in connection with company restructuring proceedings, shall be sentenced, unless a more severe penalty for the act is provided elsewhere in the law, for violation of a business secret to a fine or to imprisonment for at most two years*

Coskun & Jacobs (2003) are trying to reason the ascending problem of trade secret theft by introducing primary forces behind corporate espionage. Traditionally international trade had an emphasis on comparative advantage, but nowadays it has moved towards vigorous competitive advantage. It seems therefore, that superior market performance has become the number one target of countries and companies all over the world, thus incentivizing corporate espionage, since a company without expertise cannot survive. The recent change to information society is another fundamental aspect why corporate espionage is profitable. Competing in an information society requires long research and development processes. Less experienced companies may have to resort to espionage, since they lack the time, resources, or technical know-how to maintain long development processes. Some countries even lack the whole culture of innovations and R&D. Globalization has also enforced the activity of corporate espionage, since information and know-how flows through cyberspace from country to another. Globalization is also enabling global actors to compete with foreign and smaller companies. (Coskun & Jacobs, 2003, 98-101) Because of the global competition and technological change during the Information Age, information has become a valuable currency (Kramer, Heuer & Crawford, 2005, 14).

According to Fink (2002), the most endangered companies –target wise regarding to corporate espionage– are the ones that have introduced an entirely new industry or technology from scratch. Sometimes the simplicity of a product can affect the attractiveness of espionage activity. Companies, that invest huge amounts on research and development, are in danger as well. This makes sense, since trade secrets that are stolen or copied, are usually technology related. The corporate espionage related attacks are done to attain economically valuable information, and to copy the activities of another company; hence, the target companies are usually prosperous and successful within their area of business.

There are some characteristics of typical corporate espionage actors. The mischievous companies that commit the trade secret thefts are usually lagging behind in technology in contrast to other players in the market, and especially in contrast to the target organization. Many times a typical malicious company is financially struggling during the time of espionage activities, and that can be a consequence of poor level of competitive technology. The offender is often in a position of uneasiness regarding to competition in the market. A small player in a low-tech market might fear for global and big industry leaders who are able to deprive their livelihood with an entrance into the market. The foreign small players might think that stealing secrets is the last hope to survive. (Fink, 2002) Competitors are not the only source for corporate espionage attacks. The attacks are coming also in more "friendly" ways, which are the on-site contractors, strategic business partners, vendors, and suppliers construe a large threat to trade secrets as well. These malicious insiders will be discussed in the chapter 3.3.

2.3.5 Cyber Espionage

Amateur hackers are capable to paralyze large corporations, and steal valuable information for the sake of fun and challenge of it. However, the bigger threat to the corporations is the unethical organizations that are trying to steal the valuable information with economic incentives. The malicious stealing of trade secrets and other valuable data is today typically done over the Internet. (Fink, 2002) The term *netspionage* derives from the activity, where experienced professionals make their living by stealing trade secrets from other organizations (Fink, 2002, 123). The practitioners of netspionage are also using amateur hackers to complete the malicious attacks. These attacks are planned and financed by the actual spying organization, even though the particular spying action is done by a third party. Therefore, if the hacker gets

caught, nothing links the attack back to the real corporate spy. It might be even possible, that the hacker who is committing the action is not even aware of the organization or person paying him. (Fink, 2002)

The U.S based organization InfraGard, which is a partnership between the Federal Bureau of Investigation (FBI) and various private sector organizations, has listed three types of netspionage attacks in order to prevent hostile acts against the U.S.:

1. *Unstructured threats, encompassing threats or attacks generated from insiders, recreational hackers, and institutional hackers*
2. *Structured threats, emanating from organized crime, economic espionage from competitors, and terrorists*
3. *National security threats, coming from the intelligence agencies or other countries and so-called information warriors*

(Fink, 2002)

2.3.6 Legal Ramifications & Prosecution

Organization's IT department is closely related to the protection of organization's valuable information assets and intellectual property. IT department alone cannot do much to mitigate the risk of corporate espionage. An important part of enhancing security is to align the legal department to the risk management process. The growing amount of regulation obligates companies to protect information, but the regulation alone will do nothing, since the IT department holds the technical skills to implement the everyday privacy regulations with technical tools. In consequence, IT people and legal counsel people need to come together on the issue, to form a comradeship to assist and better understand each other. (Burgess & Power, 2006) The same problem of language has been observed between the IT security folks and executives (Cole, 2012, 43). It is apparent that illegal transfer of technology is a serious threat to organizations, and it is difficult to comprehend, since it transcends several disciplines, professions and professional communities (Reisman, 2006).

The crimes that take place in cyber world are substantially different than other "normal" crimes, and most economic crimes nowadays have a cyber-version. In addition, some nations

do not recognize the grave threat of internet-crimes to their society, and these nations have weak laws, or no laws at all, against Internet crimes. The prosecution of an Internet crime can be considered extremely complex and troublesome issue, since there are plenty of means for the perpetrator to conceal the actions or hamper the investigations. The two most problematic concepts are globalization and anonymity. Internet has global characteristics and it enables communication and data movement to take place beyond the borders. The borderless nature makes it hard for the state jurisdictions to prosecute international Internet crimes when they occur elsewhere. The anonymity of Internet is an essential feature for criminals. Oftentimes cyber-crimes offer larger payoffs but fewer risks of getting caught. Forasmuch the traditional crimes are investigated with fingerprints and physical evidence, cyber-crimes are more complicated to scrutinize. To begin the prosecution of a cyber-criminal, his or her identity has to be identified, and the electronic tracing procedure, which is done by searching each node of the Internet Protocol (IP) address, is not a simple task. (Nasheri, 2005, 32-34)

Regarding to trade secret theft, it is important to compare the different legal remedies of civil litigation and criminal laws. The cornerstone of civil litigation is to compensate the victim and to return the victim to a preexisting status quo. Civil sanctions solve the problem of trade secret thefts in monetary disbursements. The purpose of criminal law is to discourage undesirable acts, such as trade secret theft. The cornerstone of criminal law is the punishment that derives from violations of trade secret law. Whereas civil law defends the victim when the violation already took place, criminal law tries to prevent the wrongdoings proactively by intimidating possible criminals. The juridical protection of trade secrets derives from two different theories; utilitarian theory that sees trade secret information as property, and the other theory highlights the deterrence of descriptive acts and can be seen as a tort theory (Fink, 2002 ; Nasheri, 2005)

A problematic issue regarding to corporate espionage, especially in netspionage, is to prove that the crime took place in the first place. Is there enough evidence to prove in a courtroom, that the act of espionage took place? If a malicious competitor steals a blueprint of a product, there are ways to prove who the original creator of the technology was. However, regarding to a stolen customer list, proving facts in a legal proceeding would be next to impossible. (Fink, 2002) It is a serious risk managerial problem, that internationally operating companies do not have sufficient recourse to the law when it comes to corporate espionage and trade secret thefts. Some countries are considering planned espionage as a rational strategy for advancing

the economic growth. Domestically prosecutable espionage crimes are outside the countries reach, and the conduct is untouchable by international law. (Skinner, 2013)

2.3.7 International Law

The laws relating to cyber-crime activities vary by country, as well as the application of those laws regarding the complex technological issues of cyber-crimes (Nasheri, 2005, 43). This can be considered a challenge, since most of the cyber-crimes originate beyond national borders. A successful international prosecution requires that the perpetrator's country of origin cooperates with the prosecuting country. In order to extradite the corporate espionage criminal, his or her action has to constitute an offense in both the requesting and the requested state, hence the principle of *dual criminality*. As mentioned earlier, the laws and applications thereof, vary by country. The state of technological development influences the scope and application of cyber-crime related laws. Therefore, it is likely that a nation will not extradite a perpetrator to the victim country, nor take any investigative steps to solve the crime. Criminals take advantage of the system and seek to exploit safe havens, where the legislation is weaker regarding to electronic crimes. Dual criminality is not the only obstacle in defeating Internet crimes. Other nations might want to help the prosecution process, but the cooperation between two nations might be cumbersome. Finding technically literate law enforcement personnel in another country might be hard, since usually the law enforcement's response to rapid growth of technological crimes has been slow. Language, culture, and different political interests impose additional difficulties, and as a result, the investigation of cyber-crimes can turn out impossible. (Nasheri, 2005)

The World Trade Organization's (WTO) intellectual property treaties provide a legal framework for fair trade and competition, and it has the authority to ensure compliance with the judgments. The most relevant agreement is the TRIPS agreement, which is introduced as an effective and adequate intellectual property protection measure in its own preamble. Therefore, the WTO is the most effective international power and authority to fight the economic cyber espionage. (Skinner, 2013) However, bringing accusations to the WTO is always politically delicate matter. In addition, this would lead to a public disclosure of corporate espionage incident, which could in turn lead to victim's reduced stock prices. (Moore, 2010, 115)

Very often the main criminal is situated on the other side of the world, safe under different legislation and perhaps different business ethics. In corporate espionage cases, the original source of the crime is usually a competitor from a foreign country. (Fink, 2002) In the case of international hackers and spies, the perpetrators often act with total impunity, and some host countries may support these hacker attacks against the common enemy, and brand the attacker as a patriot or a hero. (Alexander, 2008, 83)

3 TARGETED TRADE SECRET THREATS

This chapter of the thesis introduces two major corporate espionage threats: outsider and insider threats. The unifying factor of these two attack types is that they both occur in a subtle and mysterious ways. These two threats have some similarities, since Advanced Persistent Threat attackers sometimes try to penetrate the organization with a cover job applicant (Giura & Wang, 2013).

3.1 Outsider Threat

Targeted attacks are fundamentally different than non-targeted attacks, since the recipient or recipients of the attacks are carefully chosen in these targeted attacks. The attacker chooses the targets depending on whether the target company has any valuable information that can be monetized. Definitions of targeted threats vary, but the unifying factor of the definition is the sophistication of the attackers. Some people define targeted threats as attacks that bypass the existing defenses and goes undetected. (Thonnard et all, 2012, 66) It does not matter how technically sophisticated the organization's information security systems are, they are not unbeatable to malicious attacker. Technology is an amplifier that enables employees to work more efficiently and accurately. Technology is not a solution for security problems, since the human behavior is responsible for the most of the security incidents relating to valuable data. (Finney, 2014)

In this chapter, I will introduce the nature of a particular targeted threat from the outside of the organization's perimeter –Advanced Persistent Threat (APT). Even though APT attacks sometimes take advantage of the organization's own employees (Giura & Wang, 2013), I will categorize advanced persistent threat as an outsider threat, as opposed to insider threat, which is the subject of the subsequent chapter. Since there are myriad of information risks and cyber threats to organizations, I will especially outline the differences between traditional cyber-attack and the APT attack. I will not only introduce the differences of the methods but also the differences in motives, actors, targets, and attack vectors. I will concentrate on the human element of advanced persistent threat, which is the social engineering. However, I will quick-

ly outline each phase of the advanced persist threat, emphasizing the non-technical attack vectors.

The main objective of this chapter is to introduce the concept of social engineering, which is an essential part of a targeted threat. Social engineering is a dangerous threat to organizations, and this threat should be identified and assessed effectively. In prior risk management books and cyber security literature, the social engineering risks have not received enough attention.

3.1.1 Advanced Persistent Threat (APT)

Organizations know how to defend themselves against traditional cyber threats with traditional security controls and software. However, defending against traditional threats is easier and more straightforward than to defend the organization's valuable data against stealthy, targeted, and data focused attacks. These attacks are named as Advanced Persistent Threats (APTs). In his book (2013), Cole states traditional cyber threats being equivalent to common cold, whereas APTs are the cyber cancer or a silent killer of the organization. If an organization waits until there is a visible sign of an APT, it is usually too late. This is why organizations have to understand the nature of APTs, and approach the issue in a new perspective. The stealthiness of APT is a dangerous quality, because an organization can focus all its energy towards perceived threats, and still get compromised. The objective of an APT attack is to steal data assets, especially targeted information or specific data. However, in contrast with traditional theft, during an APT attack the perpetrator only copies the files, leaving the original files still available to the owner. This makes it very difficult to notice a theft of any kind. (Cole, 2012 ; Ask et all, 2013)

Advanced Persistent Threat is described by National Institute of Standards and Technology (2011), as follows:

> *An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (eg, cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or im-*

> *peding critical aspects of a mission, programme, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives.*

(fismapedia.org)

In the description above, we can observe that these attacks occur in both cyber and physical world. This quashes the common belief that cyber security is technical issue. Therefore, IT department alone cannot thwart the cyber attacks. APT attack often includes actions of deceiving a particular person or a group of persons. Hence, the deception and physical attack vectors are highly important parts of cyber security. According to Thonnard (2012), APTs have a low level of sophistication, and therefore the attacks rely more on social engineering techniques.

Targeted attacks, such as APTs, can target many people in multiple organizations. However, it is more common, that APTs target only one specific company. Stealing valuable information with large-scale targeted attack is defined as "Massive Organizationally Targeted Attack" (MOTA). These attacks are as much targeted and well resourced as individually targeted attacks, but they use a same campaign to mislead the targets. MOTA attackers usually target companies in a same industry, and not necessarily in a given country, since the attacks can be multilingual. (Thonnard, 2012)

A recent example of extremely sophisticated cyber espionage attack is the "AutoCAD/Medre.A" worm, which is a MOTA attack. The malware is targeting computer-aided design (CAD) software AutoCAD, which is widely used in designing 3D blueprints of constructions. This malware has copied tens of thousands of blueprints from various engineering companies. When the victim organization is infected, the malware automatically copies CAD designs, and sends the stolen intellectual property via email to the malware operator. The malware has targeted companies especially in South-America, and the drop sites are situated in China's network, and the Internet resources were Chinese. (mytechguide.org, 2015)

3.1.2 APT Attack Types

During the attack, and especially in the intrusion part, there are usually no visual signs of any attack. APTs are designed to sidestep organization´s technical countermeasures, such as firewalls, intrusion detection systems, and anti-malware products. According to Tankard (2014), APT attacks can be characterized by their multiple means of breaking into target organization, such as social engineering, zero-day malware, trojans, and compromised hardware. Zero-day vulnerability is an exploit that has not previously been realized.

The first letter in the APT stands for *advanced*. This means that the attackers are advanced by definition, but the attack methods are not automatically advanced. Attackers often rely on social engineering methods to trick victims into installing malware. This is faster and easier way to penetrate in to the network, since developing complex malware might take a lot of time. However, attackers are able to design their own tools for the attack, and they can utilize different kind of network intrusion technologies. The attackers are well funded, and their performance is well organized. The second letter in APT stands for *persistent*. The attacks usually take long time to complete, and the perpetrators are not looking for opportunistic goals in any organization. Instead, they have a specific target and task to complete. Attackers are not interested in immediate gains, and they are ready to maintain presence for extended period of time within the network of the organization. The third letter of the APT stands for threat. The purpose of the APT attack is to steal valuable data from the organization, and this is very likely to cause financial and reputational damage to the organization. (Giura & Wang, 2013, 95 and Thonnard et all, 2012)

In order to accomplish a successful attack, the attacker has to go through various steps in the course of an APT attack. One of the key elements of an APT is the comprehensive management of the attacker´s procedures. Each step is implemented in a precise manner, and they are executed in a logical sequence. The elements of an APT attack are usually similar, even though there are usually no identical attacks, except the Massive Organizationally Targeted Attacks introduced earlier, which are less common. To exemplify the magnitude and divergence of APT attacks, the attacker may use various planes or levels in the organization's perimeter. Perpetrators can penetrate the organization for instance by breaking into a building physically, move closer to the targeted information through social engineering, and exfiltrate the information within the network level. This is an example of attack with three planes,

where the attacker is exploiting physical, user, and network planes. (Giura & Wang, 2013, 95-96)

3.1.3 APT Attack Process

There are various phases in an APT attack, and generally these phases include reconnaissance, initial intrusion, establishing backdoors, obtaining credentials, installing utilities, and data exfiltration. However, it is common that an attack does not include all the steps. APT attacks are almost always unique, since they are all uniquely outlined by the target organization's defense. One thing that they all have in common though, is the careful implementing of these aforementioned phases. In the following chapters, the most important phases and elements of the APT attacks are introduced. (Cole, 2012, 26) The focus will be on the non-technical phases of Advanced Persistent Threats.

Traditional cyber-attacks, such as widely distributed worms, do not scrutinize their targets. The traditional attackers invade on random targets, relying that at least some of them has significant vulnerabilities where the malware can break through. This is why traditional attackers do not care which organizations they get into. The only objective is to break into some organizations, and spread the mischievous code. Quantity of is usually more important to traditional attackers than quality. APTs however, need to know a great amount of the target organization, in order to compromise any valuable data. Therefore, perpetrators who execute APT attacks, spend months or even years studying the target organization in advance. The perpetrators are dwelling extremely deep while trying to understand the tendencies and key concerns of the target organization. The attacker wants to get familiar with the target systems, processes, people, and behavior of outside contractors. The quality of the reconnaissance part of the attack often determines the success of the APT attack, because the more information is collected, the easier it is to penetrate the target. It is not unusual that the mere reconnaissance part of the attack take months or years. (Cole, 2012 ; Finney, 2014)

The reconnaissance includes gathering information about the resources, employees, and the relationships of the organization (Giura & Wang, 2013). The necessary information is usually collected from the Internet, especially with the help of Google Alerts, where the attacker can easily subscribe and follow various exposures of information about named persons (Cole,

2012). Reconnaissance involves gathering public information about the operations of the target organization. Attackers have to identify, who are the most important persons in the organization concerning the access to valuable data. Those persons are deployed when delivering exploits and phishing attacks against the organization. Organizations today are revealing unintentionally large amount of information about their operations and employees in announcements, press releases, and news articles. In the reconnaissance part, the attacker usually does not interfere with the systems of the organization, so the reconnaissance part is impossible for target organization to detect. Attackers are performing correlation analysis to the gathered information in order to compose a plausible attacking plot by learning about persons' jobs, interests, and co-workers. (Cole, 2012)

Attackers, who are doing research about possible target employees, are collecting large amounts of information with the help of online social media (OSM). The Information from OSM sites does not have to include organizational information, since facts about employees' personal life is valuable as well. Private information from OSM sites can be used to guess passwords and user credentials as well, especially in the case of open profile. (Molok et all, 2010, 74)

After the attacker has enough information about the target organization, it will continue to the second part of the attack –scanning. The scanning part involves finding out specific information about the vulnerabilities in the organization's defense. This part of the attack is sometimes more technologically orientated than reconnaissance. Scanning involves finding active visible systems and open ports from the network of the target organization. Many APT attacks do not include scanning part, since it is traceable through logs, and the objective of the APT is to be stealthy as possible. Scanning may also take place in a more traditional form, such as gathering information through phone calls and physically visiting the organization's premises. However, there is a danger that scanning a target will uncover the attacker. (Cole, 2012) This part of the attack is described more precisely in the social engineering chapter 3.2.

In the next phase of the attack, the adversary is trying to obtain a foothold in the organization, and this phase often includes exploitation and compromising information. The exploitation part of the attack is all about creating a Command-and-Control connection to the victim´s computer. With a Command-and-Control connection, the attacker is able to control the target computer. This is the part where potential malware is installed or activated. The objective of

the exploitation is to stealthily collect information of the security configurations, passwords, usernames, and user e-mails. (Giura & Wang, 2013)

If the first two parts of the APT attack is done properly, the success of the exploitation part is almost guaranteed. APT attackers are sometimes using zero-day exploits when they are attacking the target organization. These exploits are sophisticated and far from easy to find. E-mail is by far the most common entry vector for a compromising malware, however not the only one. A well-designed e-mail with a malicious attachment is the most efficient and easiest way to infiltrate an organization. (Cole, 2012, 57) In the following figure, we can observe the most frequent file types of malicious email attachment.

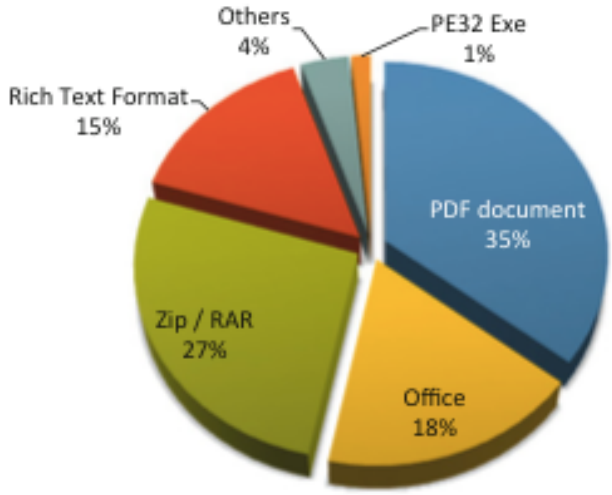

Figure 3: Most frequent malicious document types in email (Thonnard et all, 2012, 71)

The final steps of an APT attack are exfiltration and covering tracks. At the exfiltration stage of the APT attack, the perpetrator is already inside the organization's network and exploiting its vulnerabilities. However, the operation part of the attack is not a quick step, since the perpetrator might have to stay in the organization's network over long periods of time in order to collect and export the targeted data assets. During the operation phase, the perpetrator attempts to target more people inside the organization, for example with new spear-phishing emails. Spear-phishing emails are detailed phishing emails that have a specific target. This is how the offender might gain more access to the sensitive data assets. (Giura & Wang, 2013)

The attacker has an important motive to keep an access to the organization's network for extended periods, since in the cases of corporate espionage, it is more beneficial to the attacker the more time they can steal the valuable information assets (Fink, 2002). Therefore, perpetrators often create a back door in order to intrude the network in the future more easily (Cole, 2001).

The perpetrator has to effectively cover the tracks of the attack, and do what ever it takes to avoid the detection. Otherwise an APT is not successful. The attack cannot raise any suspicions inside the target organization. A perpetrator usually covers its tracks by letting the administrator believe that nothing has changed in the network during the operational part of the attack. The most common way to cover tracks is to manipulate either the system logs, the target files that have been copied, or the network traffic. (Cole, 2012)

Sometimes APT attackers conduct test runs to ensure the quality of the attack methods. This way the attackers can detect flaws in the attack, and also see if antivirus programs can detect the attacks. (Finney, 2014) The difficulty of covering tracks is minimized, when perpetrators use only user plane in the intrusion. Telephone calls do not usually leave traceable logs, if at least some precaution is applied.

3.1.4 APT Targets

The targets and the motives of APT attacks have changed over time. The advanced persistent threats used to have an impact only to military targets, and the motives were purely political. However, the targets today are mainly private corporations and the motives are financial. (Giura & Wang, 2013) In the following figure 4, we can observe the most common targeted sectors from the year 2011 targeted threat analysis by Symantec. Government & diplomatic organizations is the largest targeted sector, but private corporations together form the majority of the targeted organizations.

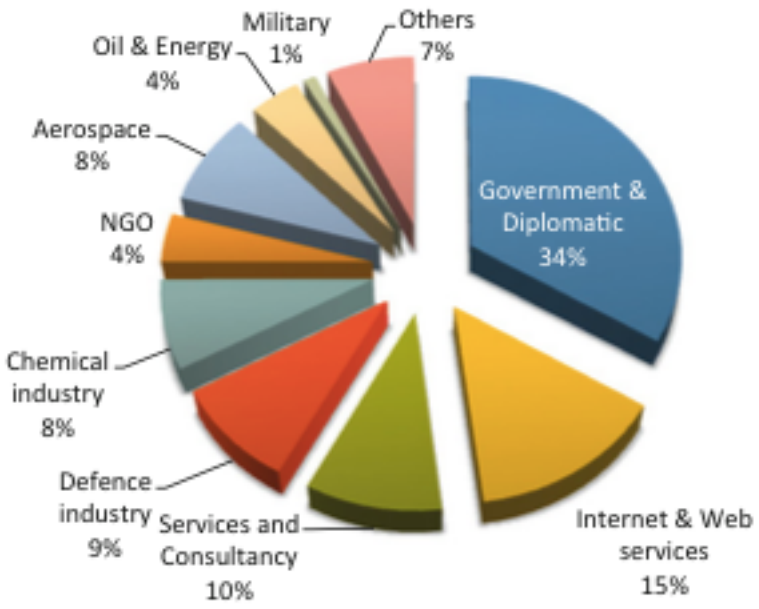

Figure 4: Top targeted Sectors from Symantec analysis (Thonnard et all, 2012, 71)

According to Cole (2013, 52), and as illustrated in the figure 4, organizations are today more common targets than states, and the persistent attackers will bypass even the most sophisticated security controls. The attacks are usually done for monetary reasons, and specially to obtain critical intellectual property from the target organization. APTs are targeting high-value individuals inside the organizations. Attackers are after sensitive, confidential, financial, and proprietary data, which these high-value individuals have access to.

3.2 Social Engineering

The area of social engineering can be considered one of the blind spots that exist in the field of information security. People and employees especially, are the biggest vulnerability, and no matter how much an organization is investing in technical security, those measures do little if any mitigation to the problem. (Rogers, 2007) Social engineering is a complex concept, which is often misunderstood. Social engineering is not an instrument, which is only used by criminals. Ordinary people use it all the time in politics and everyday situations. It also happens in marketing activities. Manipulating is a closely related term to social engineering. So-

cial engineering is a tool where the actor or group of actors is trying to skillfully maneuver the actions of human beings. There are various kind of people who are using this tool, but the basics behind the tricks are very similar. Social engineering is not a simple tool or one given trick. Instead, it is a collection of different kind of skills that are carefully implemented in a correct sequence. Sometimes the objective of social engineering is malicious and sometimes not. (Hadgany, 2010)

Social engineering can be considered an art of deceiving humans. Malicious social engineers execute attacks on information systems exploiting vulnerabilities that involve human nature. It is often stated that the weakest link in cyber security is the human operating the system. A functional system cannot be 100 per cent secure, and the human elements of the system are the easiest to circumvent. Software developers are constantly trying to secure their programs, and antivirus software companies are doing their effort to mitigate the risks of cyber attacks. Therefore, attackers are looking for vulnerabilities in the behavior of the people who are using those programs. (Hadnagy, 2010 ; Hoanca & Mock, 2008) Organizations have acknowledged the risk of social engineering for long, but the problem has still been ignored. The reason for ignorance might be the lack of hard data or metrics of the social engineering risks. Without the statistics and estimated costs it is difficult to address the issue to the executives in charge. (Rogers, 2007)

In these following chapters, I will closely examine peculiarities of social engineering and how the malicious manipulating works. I will focus on information gathering, as well as the elicitation and pretexting. Since this thesis is about risk management, I will emphasize on the negative and malicious aspects of social engineering and how to recognize the most important traits of the activity. I will outline different tools that are used in social engineering, as well as strategies and psychology behind social engineering. Upon describing the peculiarities and extreme ways of social engineering, I will also bring forward the link between social engineering and cyber security.

3.2.1 Social Psychology

Social engineering affects people in many different ways, and the psychology behind social engineering is a tortuous subject that entails individuals' feelings and behavioral traits. Ac-

cording to Hadnagy (2010), “communication entails interactions between at least two agents, and can be perceived as a two-way process in which there is an exchange of information and a progression of thoughts, feelings, or ideas toward a mutually accepted goal or direction.” According to Wood (2001), individual’s motivation and ability to process information affects to the targets attitude (Rogers, 2007). Humans have a personal space around them, both physical and mental one. People allow others to enter their personal space via communicating in order to exchange information with each other. The objective of a social engineer is to alter the target’s perception and attitude, and to use communication to create a common goal. (Hadnagy, 2010)

Humans are easier targets than computers. This is due to the fact that most humans do not think rationally and logically all the time. Humans let emotions in control, and this makes them easier to be deceived. Attackers can use social psychological weapons to trick targeted people to behave as desired. A significant risk to organizations is that people always overestimate their capabilities to detect lies. Humans are also naïve when they think that bad things, such as targeted social engineering, happen only to the others, and not to themselves. (Nohlberg, 2008)

Humans operate in one of two modes of thinking, heuristic or systematic, depending on the effort that is needed in a given task. The mental energy required in each modes of thinking is different, since heuristic thinking does not involve any effort or critical analysis. The dangerous threat, owing to social engineering, is the common habit of multitasking at workplaces, since doing many tasks at the same time forces human brain to use as little of cognitive energy as possible. Employees become more susceptible to errors and targets of social engineering, since their work is based on many different ongoing tasks that require only heuristic thinking, and there is no time to stop analyzing things systematically. (Rogers, 2007, 2899-2901)

The human element is important factor in managing targeted cyber threats. Attackers are trying hard to gather information about the employees. Afterwards, attackers use that information to influence, deceive, and manipulate employees to get access to valuable information. Humans in general are prone to be helpful towards others; hence, the simplest tool of social engineering is just asking. However, attackers have a set of means to influence the targets as

well. People are more easily influenced and manipulated when the attacker is molesting the target with certain artifices. (Nohlberg, 2008)

The attacker can use authority to enforce obedience in the target. This can be done by playing a part of a superior to the employee or by using uniforms. Faking authority can be as simple as dressing up as a technician. People can also wear uniforms to be perceived as cleaners, and get access to organization's premises. This is a significant risk, while the cleaning workers might get access to datacenters as well. Few people in the organization know who are the real cleaners, since usually maintenance staff is employed by a subcontractor. Faking authority can also come in more subtle forms, such as dressing up as an important person, for example showing of expensive clothing and just stating false title. One style of showing subtle authority is speaking with confidence and using a lot of technical jargon and arguments supported by statistics. Showing of subtle authority can be done in person, or through a phone call. (Nohlberg, 2008) The social engineer can either act as an authority to achieve obedience, or threaten to inform on supervisors, if the victim is not following the instructions (Hoanca & Mock, 2008, 136). Manipulating with authority constitutes a huge risk to both physical security and cyber security in organizations, since employees do not dare to question authority. According to Nohlberg (2008), we have been raised to obey authority and not to question it.

Fake authorities can also use the concept of overloading, which is a form to attain authority over individuals. The attacker can confuse the target with large amount of technical jargon, and since the target individual is flooded with information, he or she cannot evaluate it, and thus merely absorbs everything that the attacker says. This may lead to a situation where the attacker is seen as a more powerful authority because of his or her perceived competence. (Heikkinen, 2006, 3)

Another common trick to manipulate and deceive people is to tell how limited and rare something is. This brings up the concept of scarcity, which is used by thieves and attackers, as well as salespeople. The persuasive salesperson is trying to get the customer to act fast, stating that the offer is available only for a short period of time, and there is not much time to think. On the other hand, the malicious attacker is obfuscating the target employee with an urgency of a technical problem, inducing the target to act in accordance to the attackers needs. Scarcity has another meaning as well. Organizations are trying to hide the valuable assets, and make the information secret by classification measures. However, forbidden and secret subjects tend to

be more attractive to curious employees and perpetrators. If an organization classifies some data as top secret, social engineers are only interested about that particular data. By classifying data, the organization is also revealing that they have valuable data that is worth protecting. (Nohlberg, 2008)

Malicious attackers may also deceive targets with the help of attractive physical appearance or a voice, and there is a risk of making *security tradeoffs* (see chapter 3.2.2) when the attacker's appearance is confusing the target employee (Dontamsetti & Narayanan, 2009). Another technique of misleading is physical imitation of the target or mirroring the personality of the target. People tend to like similar personalities, and attackers can use this liking factor to manipulate or build trust. Attacker might use similar clothing or bring up fake facts about his or her background that correlates with the target employee's background. A perfect example of similarity is sharing a common enemy, for example the employee's strict boss, or bringing out fake facts outside the work life. (Nohlberg, 2008)

The attackers might also use techniques that involve reciprocation. Malicious attacker is doing a favor to which the target employee thinks he is obligated to reciprocate with an action. The attacker might give the target some sort of privileged information, and later ask the victim some information in return. The employee then feels ashamed if he or she is not giving something in return, albeit it might endanger the information security. Social engineers are extremely skilled at influencing others to do favors for them, such as forwarding emails and faxes, or other actions that seem harmless. (Mitnick & Simon, 2011 ; Nohlberg, 2008)

While presenting the manipulating arguments, attackers can enhance the likelihood of success by adding some strong feelings in the process. Attackers can intimidate targets with a sense of anger, or use feelings of surprise or sorrow to mislead the target's decisions. For example after horrible catastrophes, social engineers can put up fake and malicious donation websites, drawing people to these sites. Hence, malicious attackers use social engineering and pretexting tactics, blatantly taking advantage of human emotions. Many times in a social engineering attack, the amount of involvement of the argument has an impact on the succession rate. The targeted victim's involvement to the subject determines how they can be influenced, since security guards and receptionists care more about the quantity of the arguments, and people with high involvement, such as system administrators or executives, are influenced more easily by the quality of the arguments. (Hadnagy, 2009 & Nohlberg, 2008)

3.2.2 Security Tradeoffs

Tradeoffs are situations that involve losing something in return for gaining something. Regarding to security tradeoffs, some actions either impair or strengthen the security, and people make these actions every day in their working environment. The reason for these security tradeoffs lies in the personal inconvenience and monetary or social cost of the action. An example of inconvenient security measure would be changing login passwords with high frequency. If an action or behavior is very inconvenient, an individual is more susceptible to make security tradeoffs, thus endangering the organization's security. Respectively, the lower the social or monetary cost of the action or behavior, the more prone an individual is to make security tradeoffs. Inconvenience and cost of tradeoffs are illustrated in graphs in the figure 5 below. (Dontamsetti & Narayanan, 2008, 31-32)

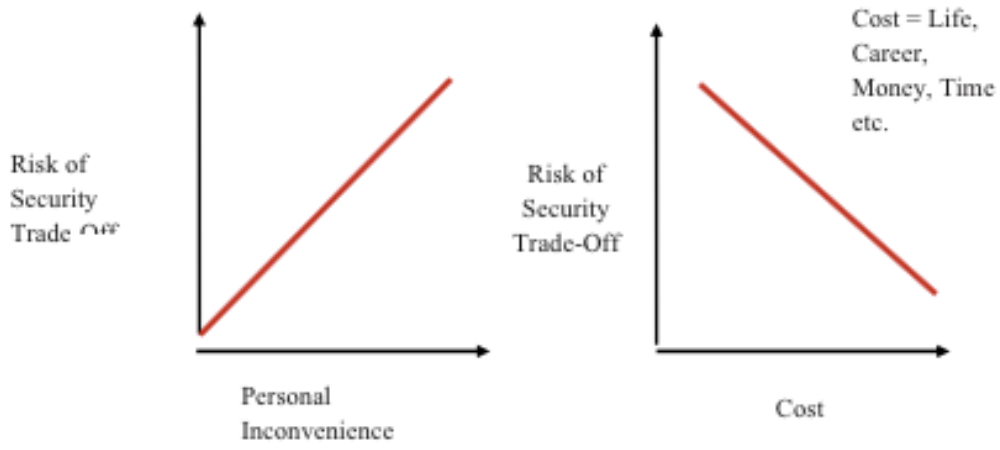

Figure 5. Security tradeoffs (Dontamsetti & Narayanan, 2008, 32)

Negative security tradeoffs are often extremely contagious. One of the most problematic attributes regarding to the human element of information security, is the social mirroring of other's behavior. This phenomenon is called social proof, where people look others for cues how to behave. Therefore, employees are copying the bad behavior of others; hence, doing the same mistakes and security tradeoffs in information security. If majority of the employees have a negligent attitude towards information security, that attitude will soon spread to decent employees as well. (Dontamsetti & Narayanan, 2008 ; Nohlberg, 2008)

3.2.3 Typical Social Engineering Attacks

Social engineering comes in many forms, and perhaps this quality makes it so elusive in the risk management perspective. According to Hoanca & Mock (2008), social engineering operations are done in person, over the phone, online, or with a combination of these forms. According to Rogers (2007), the ubiquitous telephone is usually the weapon of choice for many malicious social engineers, since there are no reliable methods of authenticating a phone caller, other than asking question from the caller. As stated earlier in this thesis, attackers from the outside, conduct a careful and profound reconnaissance before the initial contact to the organization, so they are well prepared for any questions from the targeted employees. The information gathering part of the social engineering will be introduced in the chapter 3.2.4.

As stated before in the APT chapter, targeted attacks are not opportunistic, since in the case of corporate espionage, attackers have a specific target on their mind. However, the attack methods are sometimes opportunistic, since the perpetrators are looking for short cuts and the easiest path to obtain their goals. Very often exploiting the human is the path of least resistance (Rogers, 2007, 2901). Hence, the social engineering attacks do not necessarily have to be complex, since simple measures deliver results as well. According to Dontamsetti & Narayanan (2008), a simple social engineering attack through telephone can be as following:

> *"Hi, I am your new ERP consultant and I am calling from the CFO's room. We have just finished implementing a new salary module for processing your salaries next month onwards. If you don't mind, we need your domain login ID and password to integrate your salary processing for the next month."*

The above phone call was a test done to five people, where all of the targets gave their passwords immediately (Dontamsetti & Narayanan, 2008, 30). Since the topic of the phone call was allegedly coming from the CFO's room, the social engineer was using authority as a way to achieve obedience. In addition, the subject of the call, employee's salary, was extremely personal.

According to Rogers (2007), there is no sufficient focus on the IT security controls on the phone systems, and the logging and audit capabilities of phone calls are nonexistent. In addition, the popular use of digital voice channels that facilitates social engineers to change their

voice to either be more convincing during a phone call, or alter the voice to appear different caller on subsequent telephone calls. Pretending to be different caller each time does not raise so much suspicion as a repeat caller. (Hoanca & Mock, 2008, 139)

Social engineers often use email as well. Targeted phishing is usually done with carefully structured emails or other measures of electronic communication. The objective of the phishing attacks, is to obtain sensitive information directly from the target user. Targeted phishing is usually done by tricking the user to hand over the information to the adversary through messages including a direct link to a fraud website, which is designed to harvest sensitive information, such as user credentials and passwords. Normal phishing attacks are usually launched in large amounts, since the payoff rate of the phishing attacks is rather low. Targeted phishing attacks are usually more efficient since they are tailor-made for the receiver. Targeted phishing is also called spear-phishing. (Tankard, 2011) The Anti-Phishing Working Group (APWG) defines phishing as a criminal mechanism employing social engineering and technical subterfuge to steal personal identity data.

3.2.4 Information Gathering & Pretexting

Information gathering is the initial part of the social engineering attack. The sources for information gathering are wide-ranging. Corporate websites are usually the starting point of the information gathering, and substantial amount of information can be found with search engines. On the corporate website, the malicious attacker might find out facts about the products and services of the company, physical locations, job openings, contact numbers, biographies on the executives, support forum, and special words or phrases that can help in password profiling. Some employees have a personal website where they are revealing specific details about their lives, and those details can help the social engineering process. Employees often take part in social media forums, such as Facebook and Linkedin, where they might reveal the structure and hierarchy of the department. The target company might have their own social media profile as well. Companies are publishing news and stories where the attacker might get a solid grip of the issues going on in that particular company. Frustrated employee, who is writing a blog or updating a social media status about the unfair boss or colleague, might also be a good target for an attacker, since they might share a common enemy. The more traditional information gathering techniques are dumpster diving, and overall observation of employ-

ees behavior, such as eavesdropping in company's smoking areas, and the observing the use of RFID cards. (Hadnagy, 2010)

Pretexting in social engineering means creating an invented scenario or a storyline for the malicious activity. The main objective of the pretexting is to convince the target that the malicious attacker is someone else, usually a higher authority, technical administrator, or a business acquaintance. That someone else is a character played by the attacker, who is attempting to elicit valuable information from the target employee. Pretexting is about creating a background within the bounds of possibility. The attacker creates a new identity and uses the new identity to persuade and influence the target employee. The attacker has to do a great deal of planning and practice to succeed in misleading the target. The planning includes careful information gathering about the target organization. (Hadnagy, 2009)

3.2.5 Elicitation

Elicitation is one of the fundamental parts of successful social engineering. Elicitation requires sophisticated set of skills, and it can be defined as a "stimulation that calls up (or draws forth) a particular class of behaviors" (Hadnagy, 2009, 87). Elicitation is defined by the National Security Agency as "the subtle extraction of information during an apparently normal and innocent conversation (Hadnagy, 2009, 87). In a risk managerial perspective, it is very hard to detect elicitation, since many employees run up in conversations on daily basis. Malicious elicitation can happen in bars, gyms, restaurants or a sports event and basically everywhere.

The goal of elicitation is to steer the targeted employee in some direction or sensitively force the target to take a desired action. Attacker will mislead the target by asking subtle questions during an innocent conversation. The conversation and the questions seem to be meaningless and non-threatening, however the elicitor is gradually getting hold of series of information about the target employee. (Hadnagy, 2009) A dangerous attribute in social engineering attacks is the fact that no information alone will seem to be a threat of any kind, but social engineers are skilled in aggregating little pieces of data into a comprehensive amount of information that constitutes a serious threat to trade secrets or other valuable assets. Sometimes the documents or information queried seem to be so innocuous that nobody can see any reason to

protect the asset; hence, employees are openly talking to strangers about things relating to their work. (Hoanca & Mock, 2008 & Mitnick & Simon, 2011)

In his book about social hacking, Hadnagy (2009) lists the reasons why elicitation is remarkably successful:

- Most people have the desire to be polite, especially to strangers.
- Professionals want to appear well informed and intelligent.
- If you are praised, you will often talk more and divulge more.
- Most people would not lie for the sake of lying.
- Most people respond kindly to people who appear concerned about them.

An important part of the elicitation phase of the attack is preloading, and building trust between the attacker and the victim. Preloading is about planting ideas to the head of the target before the actual conversation or intent of influencing someone. (Hadnagy, 2009) The attacker has to establish a relationship with the victim, so that they can eventually exchange information, which is the obvious goal of the social engineering. The attacker very often creates a fake problem where the victim has some sort of connection to the appearance of problem, such as guilt of committing an error that led to the problem. After such pretexting, the attacker is convincing the victim to solve the problem in sync with the social engineer. The victim of social engineering therefore believes that the attacker is a competent and friendly person who is trying to help. This blind trust may lead to disclosure of valuable and confidential information. (Hoanca & Mock, 2008) Social engineers are able to anticipate suspicion and resistance form the targets. Hence, the attackers moves resemble a chess game, where every question of the target is anticipated in advance. (Mitnick & Simon, 2011) Social engineers may build the trust and relationship with target employees during an extremely long period of time. Social engineers are persistent, so they will not necessarily ask anything immediately from the targets. (Gragg, 2003)

3.3 Insider Threat

An insider threat is an attack that emanates from inside the organization. The attacker–who is usually an employee–is a person who already has a special access or knowledge of organiza-

tion's valuable assets. Most of the times, the attacker's intention is to make money or cause harm for the employer. An authorized insider attack is someone who uses the knowledge or legitimate access against his or her employer. (Cole & Ring, 2005) The problem with the malicious insiders is that they are generally trusted, and already inside the organization's defense. In addition, insiders have significant knowledge of the organization's vulnerabilities. Insiders have also the information about organization's defense mechanisms, such as documentation policies, security controls, and the location of business-critical and sensitive material. (Rogers, 2007, 6)

A substantial part of the corporate espionage threats come from inside the organization, and those insiders are for example permanent and temporary employees, former employees, vendors, contractors, and suppliers (Kramer et all, 2005). As much as outsider threats, such as targeted Advanced Persistent Threats, insiders can as well exploit organization's valuable assets and cause damage. According to Kramer et all (2005), there are two driving forces that encourage malicious insiders to commit corporate espionage and disseminate company's trade secrets; opportunity and motivation.

3.3.1 Types of Insiders

The actions of insiders vary depending on the attacker, target, motivation, and opportunity. Each insider related trade secret theft is unique, but Cole & Ring (2005) describe three different categories of malicious insiders; self-motivated, recruited, and planted. Self-motivated insiders do not require external incentives to carry out corporate espionage against their own employer. These insiders have their own motivation to commit the crime, whereas the second category, the recruited insiders get their motivation outside. These employees are convinced to commit the crime with financial benefits. Sometimes the attacking organization can force the recruited insider to collaborate. The malicious party can for instance threaten to reveal embarrassing information about the recruited insider. The insider might end up in a situation where he or she has to decide, whether to ruin his or her personal life or hurt the company he or she works in. The third category, planted insiders, is more sophisticated than the other two. Planted insiders are people who are trained by the spying organization, and planted afterwards into the target organization. The planted insider is going through the official recruitment phase, and the malicious organization is training the insider for that. After the employment

phase, the planted insider earns the trust of the employer, and then starts to abuse the access rights to exfiltrate valuable data. Planted insider attacks are extremely persistent and advanced.

Malicious insiders can also be categorized by other attributes. Determining by their level of access and motives, there are four general types of insiders; pure insider, insider associate, insider affiliate, and outsider affiliate. Pure insiders are people who have the legitimate access to the organization's network and keys to the organization's facilities. Pure insiders are often employees, and they have the access due to their position in the organization. Some employees, such as system administrators and executives, have additional privileged access to organization's trade secrets, and those people can be considered as elevated pure insiders. In contrast, insider associates are the people who have legitimate access to the facilities of an organization, but they do not work for the organization. They might have limited access to organization's network as well. Insider associates are service providers such as guards and janitors, as well as other on-site workers, such as lawyers and consultants. Insider affiliates are people who do not possess any legitimate access to organizations facilities or network. They are friends, spouses, relatives, and clients of an employee. Insider affiliates can obtain trade secrets or other valuable information with the intentional or accidental help of the employee. Outside affiliates are outsiders, who are using open access to organization's network. An organization might have unprotected wireless access point, or employers might reveal valuable information in universities, fairs, and like. (Cole & Ring, 2005)

Malicious insiders can be categorized also by their capabilities to cause harm to an organization. Moore et all (2010), have identified that certain factors indicate a person being a "good" insider. First of all, a good insider has intention and motivation to commit the trade secret theft. Secondly, a good insider has knowledge about the target organization–often his or her own employer. The knowledge is usually associated with underlying business IT platforms and IT security controls. Insider's knowledge is an important attribute in assessing the dangerousness of the insider. Technically skilled insiders are able to steal organizations trade secrets, and conceal their actions.

3.3.2 Insider Opportunity

As mentioned earlier in the first chapter of this thesis, information technology (IT), which is improving employees' efficiency, has also dramatic consequences regarding to corporate espionage. IT has facilitated the work of a spy, owing to increasing network of electronically searchable databases. Malicious insiders are able to locate, duplicate, and distribute immeasurable amounts of files from their own workstation, and disguise the activity as a normal work task. (Kramer et all, 2005 ; Nasheri, 2005)

The increasingly competitive and rough global economy has changed the markets of stolen trade secrets. This has effects of course in outsider threats but in insider espionage as well. The demand of proprietary information has increased substantially, since trade secrets can be sold to broader range of entities. Again, trade secrets are a valuable new currency worldwide, and therefore more types of information can be sold to more types of buyers. Possible buyers include multinational corporations, research and science centers, freelance agents, terrorist organizations, revolutionary groups, drug syndicates, and organized criminals. This is increasing the threat of insider espionage, since malicious insiders have more options where to sell trade secrets, thus more opportunities to gain extra profit. (Kramer et all, 2005)

Companies are building business relationships and partnerships that transcend national borders. This is done by consolidating resources, and sharing R&D costs with joint ventures and joint research projects. This means that company's personnel are visiting other countries' organizations where malicious insiders can search for potential buyers of proprietary information, and buyers can recruit employees to become insider spies. However, it is genuinely hard to distinguish normal business relationships from possible malicious activity, since the frequency of international business travel and meetings with other companies are high. Nevertheless, perhaps the most threatening risk that provides opportunities for insider espionage is the expansion of the Internet. Internet provides brilliant venues of communication for buyers and sellers of trade secrets. Internet offers anonymity to some extent, and enables transmitting large quantities of information. (Kramer et all, 2005)

Some malicious insiders are extremely determined, and they will continue their efforts as long as they succeed in their mission. They are persistent and therefore more serious and dangerous threat to the organization. As opposed to determined insiders, the other category of insiders is the opportunistic malicious insiders. Opportunistic insiders are committing trade secret thefts alongside their work, since they notice an easy opportunity to gain money by selling

proprietary information or revealing valuable information to parties involved, such as competitors. (Kramer et all, 2005)

3.3.3 Motivation of Insiders

Malicious actions done by insiders are driven by the opportunity and personal situation of the insider. Motivation is an important cornerstone of evaluating the insider threat. Motivation is a feeling that influences people to commit actions. The experience of personal difficulties leads to higher motivation to deceive the employer, and many times these difficulties relate to financial problems. Examples of financial difficulties often relate to gambling addiction, substance abuse, loss of job, divorce, unexpected expenses, and accumulation of consumer debt. Troubled employees are motivated by the desire to alleviate their problems with a quick profit. Trade secret theft is not the only way that troubled employees try to remedy financial problems, since traditional theft and embezzlement of company money can alleviate the aforementioned problems as well. (Kramer et all, 2005, 12-14) Employees who are going through stress and financial problems are more susceptible to seize an opportunity when a malicious competitor is approaching the person with trade secret inquiries. According to an Insider Theft Study by National Threat Assessment Center of the United States Secret Service and the CERT Coordination Center (CERT Study), 27 percent of the malicious attackers were going through financial difficulties, whereas 81 percent of the insiders were motivated by financial gain. Other motivator worth mentioning is vengeance towards the employer. (Cole & Ring, 2005)

Disgruntled employees are a huge risk to a company, and the risk is extremely topical in today's business world. Organizational loyalty is diminishing because of the job-hopping through various workplaces, especially in the IT sector. Disgruntled employees are prone to commit crimes against their employer, and these attacks can be described as work-place revenge attacks. Organizations today are downsizing people and restructuring organization more often, and long working histories with the same employer are getting rare. This has led to a situation where neither employees nor employers expect long-term loyalty, and employees and employers are seeking short-term benefits and contributions. Therefore, the organizational loyalty has diminished, and mistrust has replaced fidelity. Disgruntled employers can

rationalize the crime more easily, since they feel like their employer deserves the attack, and the disgruntled employees deserve more profits. (Kramer et all, 2005 ; Nasheri, 2005)

Another source of motivation is the emotional ties to some foreign country or company. A malicious insider might feel honored to disclose information to a high ranked official or executive of his or her home country. (Burgess & Power, 2011)

3.3.4 Peculiarities of Insider Attacks

The organizations that are willing to steal proprietary information and valuable assets, may as well use personal vulnerabilities of the target company's employees. Some people have dark backgrounds, which they want to protect. An external party, such as a competitor, can leverage the employer to cooperate in trade secret thefts by threatening to reveal the secret. (Cole & Ring, 2005. 44-45)

The earlier introduced Insider Theft Study reveals interesting details about the features of malicious insiders and their behavior. According to the CERT study, only 23 percent of the malicious insiders were from technical positions. Therefore, the typical insider is a normal worker with normal technological skills. Most of the malicious insiders have 3 to 5 years of working history, so they are considered trusted entities. In 85 percent of the incidents, a third party knew about the forthcoming insider attack, and of those cases, 22 percent of the times it was a coworker, and in 22 percent of the cases as well it was a friend or a family member. It is impossible to find any indicating personal traits regarding to malicious attackers, since insiders who were caught vary in social background, age, sex, and education; hence, there is no single profile for the attacker that would help to identify the malicious insiders. However, 27 percent of the caught insiders had previous criminal history, and many times the employer was unaware of the criminal records. This indicates that organizations are not doing enough background checks to their employees. (Cole & Ring, 2005)

There are basically three ways the insider attacks effect on a company, depending on the actions of disgruntled employee or other insider. One way to harass an employer is to destroy or modify company's valuable data, so that the data is no longer usable. This action is called sabotage, and it causes the mildest effects to the victim organization of all the three attack

types. Disgruntled insiders who undertake actions of sabotage, often want to take credit for their actions, and usually perform the attack only once. The attack causes financial losses, but indirect losses are limited. The second attack type, modifying the company's intellectual property, is more disguised and threatening, since the objective is to hide the sabotage from the victim. These types of attack are usually causing malfunctions, and may lead to abolishment of the use of particular intellectual property, benefiting the competitors. Finally, the most dangerous form of insider threat is the trade secret theft, where sensitive intellectual property or other trade secrets end up in the hands of competitors. (Cole & Ring, 2005, 21)

Insider threat cannot be considered a technical issue, and being a malicious insider does not require any hacking or sophisticated technical skills whatsoever, since according to the CERT study, in 87 percent of the cases insiders used simple and legitimate user commands to execute the insider attacks, and in 43 percent of the cases, the insider used his or her own passwords to commit the crime. The same study revealed some other interesting results from the incidents, for example that 83 percent of the thefts happened in the employer's premises, and 70 percent occurred during working hours. (Cole & Ring, 2005)

3.3.5 A Case of Insider Attack in Finland

An example of a corporate espionage done by malicious insiders is illustrated in a legal case of the Supreme Court of Finland. In the instance, prosecutor was demanding a punishment for two employees for an attempt of corporate espionage, where the plaintiff was operating sales of IT products and professional services. The defendants were accused of copying customer related databases to an external Hard Drive on the verge of switching workplaces to a regional competitor where the accused employees would have allegedly used the stolen files. The negotiations of changing workplaces occurred few months before the copying of over 10 gigabytes of confidential files. The court ruled that the crime was committed during a switch of workplaces, and the wrongful act was made in several different stages; therefore, it was considered a deliberate and calculated crime. The defendants did not manage to use the stolen information, and the crime did not cause any other financial damages to the plaintiff, except the settlement expenses. Fines were considered too mild punishment, and the court of first degree (Porin Käräjäoikeus) sentenced the both defendants for four months conditional sentence of imprisonment. (KKO:2013:20)

The appellate court (Vaasan Hovioikeus) did not reverse the lower court's ruling. The determining factors were the timing of the act, and the large amount of files copied. There were no doubts that the purpose of the act was to use the databases in their future workplace. The competitor would have obtained a huge amount of useful information of plaintiff's customer database. According to the logs of the external Hard Drives and the defendants' laptop, the stolen database files were explored after the resignation of the employees. The defendants appealed to the Supreme Court of Finland (Korkein Oikeus), demanding that the ruling of appellate court should be reversed and all charges dismissed. The Supreme Court did not reverse the ruling of appellate court. However, the penalty was altered to a period of three months, and the criminal offense was eventually infringement of trade secrets. (KKO:2013:20)

The case does not specify the motives behind the crime; therefore, it is hard to categorize the insiders to any specific type. It is unclear, whether the future employer had anything to do with orchestrating the crime. However, the defendants would not have received any direct financial benefit from the crime, since the beneficiary of the files was the future employer. The future employer would have gained competitive advantage from the plaintiff's customer databases. It is also unclear, whether the defendants were disgruntled employees. However, the organizational loyalty was clearly diminished, and the crime was not spontaneous action, since the malicious insiders worked together as a team. Working as a team requires at least some amount of planning. The negotiations with the future employer were done in separate occasions, and files were copied several times as well.

4 RISK MANAGEMENT SOLUTIONS FOR CORPORATE ESPIONAGE

This chapter introduces human risk management controls against trade secret threats that are occurring in the information risk environment. The chapter includes four different sub-categories of risk management: data classification, awareness, policies and guidelines, and penetration testing. Throughout disclosing these risk measures, I will reflect the measures to the threats introduced previously in this thesis: social engineering and insider threat. Firstly however, before going into the details of these aforementioned risk controls, I will outline the relationship between information security and Enterprise Risk Management (ERM). The non-technical risk management practices for outsider and insider threats mostly fall into the category of operational risk management (Chernobai et all, 2008). Therefore, a short introduction of operational risk management is presented.

People are often stated to be the most valuable asset of a company. However, the treat may originate from the inside as well, as introduced earlier in the chapter 3.3. Having a well-trained staff is useful against both insider and outsider threats, and there are few risk management solutions than can mitigate the risk of corporate espionage. As stated earlier in this thesis, the weakest link of information security is always the human being. Large investments in technical solutions are not mitigating the risks, since there are no effective technical remedies against social engineering attacks and insider threats. Hence, organizations need to look for other controls, such as physical security, operational security, and personnel security to fight against insider and outsider threats. Physical controls are usually inadequate alone, especially when the attack is occurring in the cyber environment, since the perpetrators are usually not physically present. According to Damien (2002), there are three different steps to effectively mitigate social engineering attacks: training, policy creating, and testing (Botelho & Gazier, 2008). According to Cole & Ring (2005), the insider threats are mitigated with policies, training, and awareness. Policies are telling what to do, training teaches the skills for doing it, and awareness changes the attitude and behavior towards the problem. All the three steps are critical, although their effectiveness is best achieved when combined. Together they are able to control, reduce, and even stop insider threats, if they are implemented and monitored properly.

4.1 Corporate Espionage as an Operational Risk

Enterprise Risk Management (ERM) is a broad concept that consolidates all parts of the organization into a one single strategic risk management process. ERM provides better changes to identify, mitigate, avoid, and treat risks that are threatening the organization. ERM also facilitates the communication between different departments of the organization, as well as communication between risk managers and the board. (Hampton, 2009) Facilitated communication is extremely important in information risk management, since information risks are more difficult to comprehend. In addition, putting a price tag to corporate espionage is impossible, since there are usually no immediate costs. Therefore, different departments have to assess the risks together. Enterprise Security Management (ESM) is a closely related term to ERM. ESM program allows organizations to make better business decisions regarding to information security, and it is defined as enterprise-wide program that helps to protect organization's assets from security incidents and threats. (McBride, 2003) Top management should therefore be extremely committed to the information security policies and procedures, since a failure in identifying information security as a core competency may have a direct affect on business' survivability (Torres et all, 2008).

The non-technical elements of information risk management against corporate espionage fall into the category of operational risk management. Operational risks include human fallibility, defective processes, and unreliable technologies. Operational risks have usually low probability of occurrence but grave financial consequences. Some of the operational risks result from unintentional accidents, and others result from fraudulent or criminal activities. The Bank for International Settlements (BIS) approved definition of operational risk is "the risk of loss resulting from inadequate or failed internal processes, people or systems, or from external events", and this definition excludes both reputational and strategic risks (Chernobai et all, 2008, 17).

Traditionally operational risks have been monitored and managed informally alongside other management work, without a consistent risk managerial approach. Compliance and audit functions have traditionally been the only pure risk management process against operational risks, but this retrospective measure is not sufficient. (Lam, 2014) These episodic risk management functions cannot fight against corporate espionage, or other operational risks whatsoever, since the retrospective detection of a trade secret theft does not help to mitigate the

occurred risk. Even though the perpetrator might get caught, the trade secret is long gone, and prosecution measures are of little help. Lost trade secrets result in diminished competitive advantage. However, the major financial crises, especially the subprime crisis, have brought to light the importance of operational risks, and the issue has been addressed in the Basel II capital requirements (Chernobai et all, 2008 ; Lam, 2014).

4.2 Data Classification

Almost every organization in the world has an extensive amount of data. However, not all of the data is sensitive or valuable to other parties, such as thieves and corporate spies. Therefore, the organization has to acknowledge, what information they should protect. The possible perpetrator's objective is to extract valuable data from the organization, and monetize the stolen assets. However, an organization simply cannot stop every file leaving the organization, since it would most definitely harm or obstruct the business activities (Cole, 2012 ; Peltier, 2001). According to Peltier (2001), data classification is the solution for adequate protection of valuable data assets. Fundamentally thinking, the information classification process is a business decision process that affects the whole security, since classification process will be the base for all security policies. Therefore, the management should participate and collaborate in the process, and take policy writers into consideration in the process ass well.

In his book about advanced persistent threats, Cole (2012) outlines seven general steps of a good data classification process:

1. *Identify the administrator/custodian.*
2. *Specify the criteria for how the information will be classified and labeled.*
3. *Classify the data by its owner who is subject to review by a supervisor.*
4. *Specify and document exceptions to the classification policy*
5. *Specify the controls that will be applied to each classification level*
6. *Specify the termination procedures for declassifying the information or for transferring custody of the information to another entity.*
7. *Create an enterprise awareness program about the classification controls*

(Cole, 2012, 107-108)

Implementing an awareness program about the data classification controls is not a simple task for an organization, and many organizations make a myriad of mistakes within the process. (Cole, 2012) According to Tankard (2014), organizations first task should be mapping all data in the organization, recognizing to whom the data is available, how and where it is stored, and what policies apply to the data. In addition, the access to all confidential and valuable data should be controlled and audited.

It is essential, that the valuable data and information are classified into groups by risk. The following factors should be taken into particular consideration regarding to each piece of data:

- The decision whether the data is sensitive or not.
- The reasoning behind possessing the particular information.
- The monetary value of the information.
- Consequences of information compromise.

(Tankard, 2014, 15)

In the data asset classification process, the first rule according to Cole (2013) is to determine the amount of classification levels. The classification should at least start with two categories; eg. public and private. Too many categories might create confusion, and too strict classification might be inefficient, since the process would take more time. Another mistake is to classify all information as confidential. The classification should be easily understandable and simple. Organizations should start with the two categories mentioned earlier, and then subdivide the private information category into supplementary categories. For example, the US government agencies use three categories to classify information. These categories are confidential, secret, and top secret. (Cole, 2012) Another example of classification is the following set of categories–in descending privacy order: Top Secret, Confidential, Restricted, Internal Use, and Public. (Peltier, 2001)

Organizations have a great amount of data, yet usually little understanding about the protection measures of the data. The process of prioritizing data should start with determining the metrics. Organization must know how to determine the value of the data assets. Some data assets are of no monetary worth, but the data is anyhow crucial, since the data assets might create competitive advantage. Although the quality and usage of the information assets vary,

the valuation method must be invariable throughout the process. When the valuation criteria are alike, the organization needs to start prioritizing the data assets. The valuation process should include executives and employees from various business functions inside the organization. (Cole, 2012)

Data asset classification should also define the owner, custodian, and user of each piece of information. Information owner is the company department or other organizational unit where the information is created. Owners have responsibility to identify the classification level, and to implement the safeguards necessary. Information custodian is the person responsible for overseeing and maintaining the safeguards implemented by the information owner. Custodians can be system administrators, employees, contractors, consultants or vendors. The owner of the information entitles custodian, and the custodian will be the steward of the data. The final component in the chain, information user, is the person responsible for viewing amending, or updating the content of the information asset. The custodian is usually responsible for monitoring the users. (Peltier, 2001, 83-86) Defining information owners, custodians, and users is an effective way to clarify the roles and risk owners inside the organization. A healthy precaution should be taken when an unfamiliar party is giving orders or requesting information about valuable data assets. Multiple individuals or departments dealing with each risk in a committee, is not efficient way of managing risks. (Hampton, 2009)

4.3 Awareness

Awareness of the risks is vital to an organization's defense, since mere policies and guidelines do not offer sufficient remedies against targeted threats. Even the most complete and strict policies and guidelines may turn out useless, if the employees are not following the rules consistently. Hence, employees need to be trained to be aware of the risk, and admit the general and personal susceptibility. General susceptibility means believing that the risk can occur to others, and personal susceptibility means accepting the own vulnerabilities to the risk. Awareness training should aim to prove employees how easy it is to be fooled by a skillful social engineer. (Gragg, 2002) According to Sagarin (2002), employees' resistance to persuasive attacks depends on two critical factors; acknowledging the attacker's maliciousness, and admitting personal vulnerabilities (Gragg, 2002, 14). Awareness training is also a preventive countermeasure against corporate espionage and other information risks. Preventive security

countermeasures are cost-effective, since generally prevention costs less than curing a problem. Security awareness is also less expensive than high technology controls. According to Peltier (2005), the awareness security program must be clearly justified to employees. Firstly, the organization must communicate with the employee community, and promote the message of information security. The organization must then decide the people responsible of the awareness program, and determine the sensitivity of information (see chapter 4.2).

4.3.1 Awareness Training

Preventing social engineering attempts require a holistic security awareness program. Awareness program should include information about social engineering attacks, different types of attackers, and what social engineers are after. Fostering awareness in an organization is not an over-night job. It requires time and effort to instill itself to the organization's culture. In the beginning of the awareness program, objectives, assigned responsibilities, and management direction should be addressed. Awareness program needs to have a flexible plan, where the organization states its IT culture, current efforts towards security awareness, program goals and objectives, and schedule of the plan. (Hadnagy, 2010 ; Rudolph, 2006)

Awareness training should tackle the problem of employee attitude and carelessness about information security and confidentiality. Many employees in many organizations do not honestly care about the confidentiality or integrity of the information, since the data assets are not their own possessions. Therefore, employees do not have the personal incentives to defend the valuable information, and they are ignorant to devote time to the awareness program. (Hadnagy, 2010)

The interconnectivity of policies and awareness is crucial to organization's defense. Organization's employees should be trained and guided with strict policies to be in a position of complete confidence about the information they can share, and to whom they can share it with. There should not be a situation where employee is considering, whether to give information to a caller or not, since these questions should be addressed beforehand in policies and guidelines. Policies remove the responsibility of making judgment calls regarding possible social engineer's requests. If the employee is aware of the competent policies and guidelines regarding to giving out information, the persuading social engineer will not have any influence on

the target employee, since the employee can trust the functionality of the policy. An effective policy has an effect on how an employee responds to request, thus mitigate the risk of social engineering. (Grag, 2003, 10-11 ; Granger, 2001)

4.3.2 Awareness of the Attackers

Organization's employees should always be aware of the attackers moves. All employees must be trained to give an unconditional and prepared answer to the possible social engineer, who is requesting confidential information. This must be a simple and polite refusal, since the caller might be also non-malicious, such as an important client or business partner. Dubious callers should be instructed to contact a specific person who is responsible for administrating or safeguarding the information, i.e. the owner or custodian of the information. Employees who are receiving the rare and dubious questions must be aware that their job positions are not in danger due to refusals to give information. Many social engineers use the element of fear and intimidation by mentioning the names of the target employee's superiors. (Hadnagy, 2010 ; Peltier, 2001) Employees' strongest defense is to say no to rare requests, and to be unconditional. Employee must be absolutely certain that he or she is right, in order to have courage to refuse to answer a dubious question. Any insecurity will endanger the situation, since social engineers are prone to start negotiations with the employee, and that may eventually lead to an assent on the targets behalf. (www.t2pa.com) Policies and their obedience should be so strict and habitual that even strong emotions during a social engineering attack would not hamper the behavior of employees. According to Duhigg (2012), routines and habits provide hundreds of unwritten rules how companies operate. Routines provide "organizational memory", which reduces the uncertainty of employees in difficult situations. Therefore, companies should carefully observe the organizational habits among workforce.

One useful and pragmatic risk management solution against social engineering attacks is developing scripts. Employees could be trained for specific situations, so that they are prepared when the social engineering attacks occurs. Employees should have prepared responses for various kinds of attack vectors, for example; what to do when someone is demanding passwords or user credentials? What to ask for an unidentified caller? Script developing has two benefits. First of all, employees learn how to defend the organization during a social engineer-

ing attack. Secondly, when preparations against the social engineering attacks are developed, employees will become more aware of different kinds of attack methods. (Hadnagy, 2010)

Organization's employees should also remember the importance of reconnaissance part of the targeted threats. Malicious intruders are seeking public information from various sources, mostly in the Internet sites. Employees should therefore be careful about the content they are publishing to Internet sites. In order the social engineering to succeed, the pretexting phase requires careful research about the target, and the depth of the research has to be substantial. This is an important phase considering risk management. The exposure to this risk is manageable, since the organization can prevent revealing information that could be used against it in malicious social engineering. Too specific curriculums in LinkedIn or posting disgruntled status updates to social media sites are examples of risky behavior. Social engineers can hack accounts and disguise themselves as allies. Social engineers are able to gather little pieces of information from various sources, and employees need to be aware of this. However, controlling employees is an ambivalent issue. Organization's policies should extend to the use of social media, but policies cannot effectively control or restrain employee's activities outside work, and the social engineer can approach the target within the target's leisure activities as well. (Hadnagy, 2009).

Another risk management solution against targeted attacks is accurate verification. Employees must be aware who the contacting person is. Social engineering attackers are using pretexting and fake identities to obfuscate target employees to act in accordance with the attacker. Contactor verification is therefore an important tool in overcoming the social engineering attacks. As stated earlier in this thesis, the most common attack vector of social engineers is traditional phone call. Therefore, employees should be somehow able to verify the identity of the caller, especially if the caller is not well-acquainted. One solution is to enquire the caller with some details, although this can be seen as rude and inconvenient. The most simple and efficient way is to ask the name of the caller and the organization that he or she is representing, then call back to the organization's service center, and ask to connect the call to the original caller. This behavior is called call back policy, and it is a feasible method of verification, especially when people are handing out questionable information over the phone. If the possible social engineer denies the call back, and starts explaining why it will not work, the person receiving the call should have the freedom of not granting the information requested. (Alexander, 2008 ; Gragg, 2002, 16)

4.4 Policies & Guidelines

Implementing policies is one of the key risk management measures to mitigate social engineering and insider threats, and perhaps the most traditional of the human risk management measures. Policies, which safeguard technology and human failures, are important part of the organization's information security plan. The implementing phase of the policies is not a simple task, since policies should coalesce with organizational structure and culture. The ultimate goal of the policies is to forestall the misuse of organization's valuable data, and to prevent the compromise of information security. The misuse can be e.g. unauthorized acquisition, damage, disclosure, manipulation, modification, loss, and use of information assets. (Gupta & Sharma, 2008) Policies are also aimed to ensure the information risks: integrity, confidentiality, and availability (Hamdi et all, 2006). Regarding to trade secret thefts, the principal misuse is of course unauthorized acquisition and use of proprietary information, such as intellectual property, blueprints or business plans. Since the risks in this thesis are related to social engineering and insider threats, this section will only deal with policies that have repercussions to these human threats. Relevant to corporate espionage risks, the most important aim of the policies is to spot social engineering, and to improve the reporting standards of close calls.

Policy documents are useless, unless they are understandable, simple, and easy to access and use. (Gupta & Sharma, 2008) There are various areas, where strict policies should be implemented to protect the organization against trade secret threats, both insider and outsider threats. Policies should consider information access controls, setting up accounts, access approvals, password changes, locks, ID's, paper shredding, and escorting visitors (Gragg, 2003). However, policies are also seen as barriers to efficiency and progress, and this can lead to circumvention of the policies and guidelines (Ghormley, 2008, 321) Policies are extremely relative to awareness training, and it is crucial to acknowledge the interdependence between security policies and awareness training. Without proper awareness training, policies are generally viewed merely as impediments to the work. (Rudolph, 2006)

4.4.1 Policy Development and Implementation

Rees et all (2003) have developed a thorough multistep policy creating tool, Policy Framework for Interpreting Risk in e-Business Security (PFIRES), which is shown in figure 6 be-

low. This framework is adjusted to ensure basic requirements of information security, such as confidentiality, availability, utility, authenticity, and integrity. The security policies need to be aligned with other organizational objectives; therefore, the policies should be created together with representatives from human resources, legal and regulatory departments, and information system administrators. There are several factors that determine the quality of policy framework, and according to Maynard & Ruighaver (2006), these quality factors and measures are functionality, reliability, usability, efficiency, maintainability, and portability. However, the policy implementation should align with the organization's other activities, especially information security and risk management. The organization that is initiating a policy program, should divide the responsibilities of developing the policies. Senior management should sponsor, fund and support all policy activities, and chief information security officer (CISO), or chief information officer (CIO) should be responsible for the planning and budgeting of the process. Information security should also be in tune with risk management activities. (Peltier, 2001)

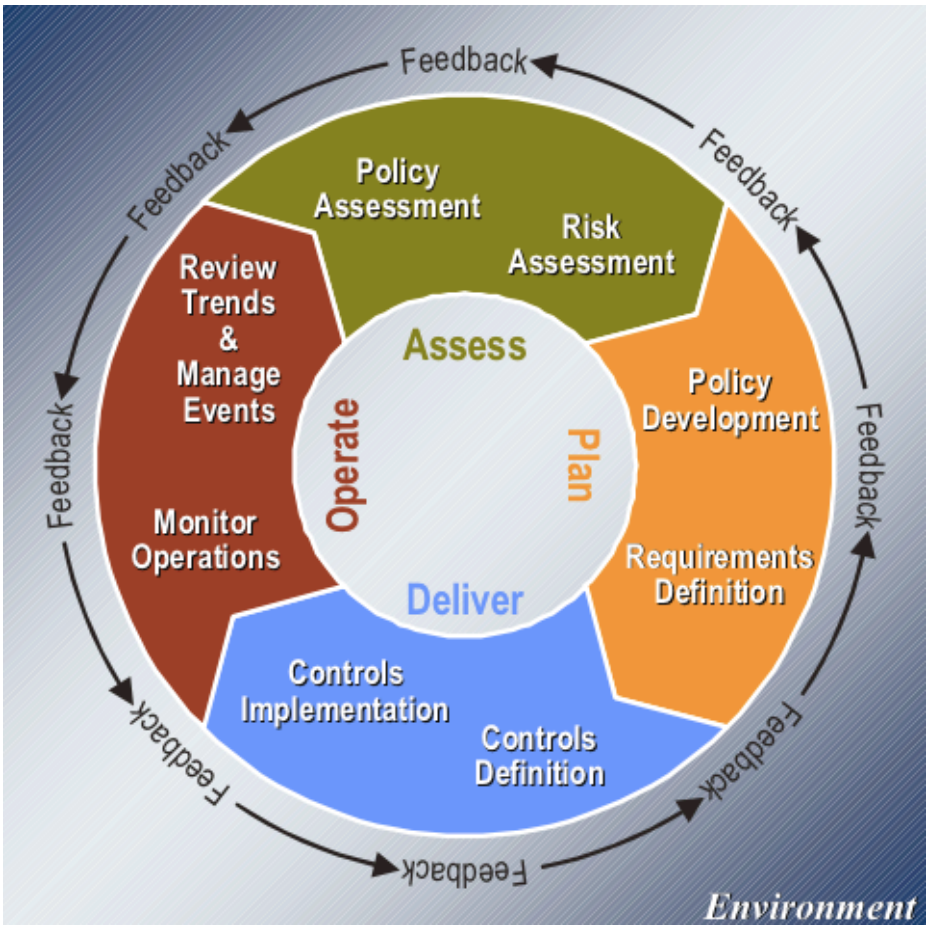

Figure 6. Policy Framework for Interpreting Risk in e-Business Security (Rees et all, 2003, 4)

The PFIRES framework, consist of four categories, which are assessment, planning, delivery, and operation. The usual starting phase is the policy assessment, which aims to assess the changes that should be made to existing policies by reviewing existing policies, standards, guidelines, and procedures. This is followed by risk assessment, which evaluates the most valuable assets that the organization has to protect and the possible threats to the valuable assets. (Rees et all, 2003) Evaluation of valuable assets by data classification was introduced earlier in this thesis, in chapter 4.2. Data classification is an important task to execute before developing policies.

The second phase of the policy creation framework is precise planning and assuring the goals of security policies. Building a policy framework should be considered as a project, and teams should develop policies and standards with established team leaders. These team members should have experience of several years within the organization, so they have knowledge about the culture of the work environment. (Peltier, 2001) According to Rees et all (2003), there are two phases in the planning phase; policy development and requirements definition. Policy development has to assure that overall security strategy and the security policies are aligned with business strategy. This may require strategy sessions with managers from various departments, to identify future business initiatives. Requirements definition is about developing detailed security requirements, and ensuring that older recommendations are translated to requirements. These requirements should represent the risks introduced in the assessment phase, and they have to be evaluated against industry best practices.

The next step of the PFIRES framework is the delivery phase, which is the actual policy implementation phase. First of all, delivery is about defining applicable controls that reduce the security risks. These controls require designing the security infrastructure, determining and selecting security controls, and evaluating solutions for each control. After the definition phase, the actual controls can be implemented. Planning and testing the implementation phase is extremely important. Planning ensures that the design is translated into reality, and testing assures that the design is properly executed, and the threats are accurately identified. The final step of the framework is to initiate the operation phase, which is basically a continuous monitoring of the policies and their adequacy regarding to possible technological or business trends in the policy environment. Operation phase consists also the handling of incident response. (Rees et all, 2003)

As stated earlier in this thesis, the perpetrators of targeted threats are extremely persistent. This means that they are trying many ways to penetrate the organization. Therefore, each and every employee, without exceptions, has to abide the policies and guidelines. Otherwise, the perpetrators will change the target employee, until they find defects in the defense. The human element of corporate espionage risk management is as strong as its weakest link. This is why organization's policy has to include an effective incident response guideline. There should be at least one employee in the organization to collect logs and incident reports from social engineering attacks. The person in charge of incident reports should categorize the attackers, and alert other employees immediately. (Gragg, 2003 ; Shaurette & Schleppenbach, 2013) According to Rees et all (2003), each and every incident or close call situation should be investigated properly by verifying the root of the cause, and all facts and people involved. Rees et all continues, that incident investigations must include the following activities;

- Documenting actions taken during the incident
- Maintaining thorough records from the incidents
- Providing information to support legal actions
- Procedures for tracing the source of an event
- Guidelines for chain of management during an incident
- Procedures for limiting the damage from incidents

Another crucial part of the operation phase of the policy implementation framework is to identify external and internal trends, especially the risk trends, such as social engineering attackers and possible malicious insider activity. If an employee notices any rare behavior that might be social engineering, he or she has to report the malicious action to other potential victims in the organization as well. Otherwise, social engineer will only gain more information about the organization's defense, and the next attack might succeed. It is important to remember that only one attack has to be successful, and the company may be shattered completely. (Gragg, 2003 ; Shaurette & Schleppenbach, 2013) Employees should also be aware of the insider threats, such as the possibility of malicious coworkers who might be stealing or planning to steal proprietary information. All employees should be trained to observe mysterious actions and strange requests done by coworkers. These actions and requests should be reported immediately to the owners or custodians of the information, such as systems administrators and managers. Therefore, the incident response instructions should be clearly stated in poli-

cies, and policies must include notification conduct in the case of possible malicious insiders. Policy writers are in a crucial position, since they need to have a complete understanding of the corporate espionage threats, since these threats have to be instilled into the policies. In addition, policy writers need to know their audience, since all the employees need to comprehend the written policies, and this requires good writing skills and knowledge of the workplace (Peltier, 2001).

Policies should never be considered static and ready, since the threats, technology, and attack vectors are evolving all the time. Organizations need to continuously evaluate their policies, and make dynamic changes to them. Security implementation processes often fail because of the understaffing and lack of personnel dedicated to information security issues, such as dynamic implementation of policies and awareness training. The ideal situation is when the organization has a qualified and highly involved security implementation team, which is constantly evaluating the accuracy of policies and the need of training employees. (Torres et all, 2008) The PFIRES policy framework is a substantial tool in developing and implementing policies, and it can significantly facilitate the communication between senior management and technical security staff. This facilitated communication alone can lead to better security, and increased protection from insider and outsider threats. (Rees at all, 2003)

There are several features that help to improve the policy framework implementation in an organization. Employees are more concerned about the security issues, the more responsibilities and varying activities they have in their workplace. As a consequence, rigid hierarchical organizations have problems implementing effective policies. (Ghormley, 2008, 322)

All employees need to abide the policies all the time, and no exceptions should not be allowed, since omission can easily turn to ignorance through social proof. No matter how excellent the security policies are, they are not functioning if some people are ignoring the policies. Even a small part of ignorers might endanger the security, since the negligence is contagious. If a security aware person enters to a security negligent community, the individual might be perceived as paranoid or untrusting among the other workers. Individuals absorb the culture of the society they live in. Therefore, it is more important to instill positive culture and security acceptance to the workforce rather than just draft strict policies. Policies should also be strict and flexible at the same time. Flexibility is important, since the trade secret thefts are unique, and their attack methods and vectors change over time. Strictness of the policies help

the staff to be alert all the time, and not to become too relaxed while performing their daily work. (Dontamsetti & Narayanan, 2008 ; Nohlberg, 2008 ; Ghormley, 2013)

4.4.2 Rotation and Separation of Duties

Although policies will never outplace the supervision of employees, they can be an effective measure to define duties, responsibilities, and authority. A well-written policy will identify who is responsible and for what activity, and policies can be source of authority when management is unavailable. Policies can also formalize duties in a more secure way. This is done by separating duties and rotating assignments. Separation of duties ensures that no single employee has complete authority or control of some valuable information or a task. (Peltier, 2001)

Rotating assignments and jobs is an effective risk management measure especially against malicious insiders. Employees have to do more effort to hide their malicious actions, if they are sharing an assignment or a position with another employee. Another individual in the chain notices mistakes made by the other employee, and this is increasing the information integrity. Respectively, another employee in the chain might notice the malicious activity; therefore, increasing the information confidentiality. Malicious insiders have harder time to conceal their actions, since at least one other person is watching over his or her actions. (Peltier, 2001, 29-30)

The other similar duty formalization policy is rotation of assignments. Some tasks in an organization are so crucial regarding to the security issues, that only one employee is not enough to ascertain the security. Rotation of assignments doctrine provides other benefits to the organization as well, such as cross training of personnel and job satisfaction. However, the most important benefit is the improved discovery of misuse and fraud. Too much rotation can lead to inefficiencies, yet while working long time with the same assignment, employees may commit security tradeoffs by developing shortcuts. (Peltier, 2001)

4.4.3 Policy Types for Corporate Espionage

One of the most commonly used data protection measure is to control the access to the sensitive data. Typically this is done with passwords and usernames. Despite the common usage, password authentication has serious flaws. The most important flaw is the human link in the security system. Passwords are created and used by humans, and those passwords are the only obstacle for perpetrators to intrude a system or database. People have tendency to use weak passwords or the same password for many different accounts. (Botelho & Cazier, 2009)

Password security is an important area of organization's risk management. Password policies are easy to address and implement, but ensuring the correct use of passwords is impossible, since passwords are private. However, employees should at least understand the privacy of passwords, and this should be included in the written policies. In an organization, nobody should ever need to ask passwords from other people, and this should be absolutely clear to everyone. (Botelho & Cazier, 2008) Organization should also have a policy that forbids the use of the same or similar password at workplace and in other sites. Social engineers can obtain employee's other credentials as well, and use them against the targets organization. (Gragg, 2003, 12)

Social engineering attacks rely often on eliciting passwords and user admins from the employees. Social engineers' actions are subtle and persistent, and they maneuver skillfully the target employees. However, if the password security policies are extremely clear and strict about revealing passwords to anyone, the social engineering attack should not succeed. Policies have to make it clear that passwords are not revealed to anyone under any circumstances.

Since social engineers may approach the targets physically, it is important not to write down the password anywhere. Malicious outsider can bypass the employee's workstation, and collect sensitive information lying around. Therefore, passwords must be memorized and kept private. Social engineers are able to use uniforms to enter buildings and sneak into places where they have no reason to be. Uniforms are cheap to buy, and uniforms have a strong effect on people. Therefore, employees should be trained to not trust uniforms and authorities blindly. (Botelho & Cazier, 2008 ; Gragg, 2003)

It is important to remember that illegitimate password inquiries may emanate from inside the organization as well. Therefore, the risk management methods should be adjusted to other coworkers and onsite contractors as well. Employees should not disclose any user credentials

to other employees, since malicious insiders can use other employees' authentication credentials to access valuable information that is not in their reach or if they want to uncover their actions. Therefore, it is crucial to notice that social engineering attacks may come from inside the organization as well. Strict policies can complicate significantly the insider attacks, especially when there are sufficient reporting guidelines. Policies need to include codes of conduct when it comes to suspicious and abnormal situations, so that incidents cannot remain in the dark (Granger, 2001 ; Botelho & Cazier, 2008). Security policies should include the statement that all trade secret thefts and offenses are reported to authorities. With this intimidation, employees might be less willing to risk their careers.

Alongside with passwords, hiring process and employee retention policies deserves to be mentioned, since these subject areas constitute such a severe operational risk to organizations. During the hiring process, the HR manager and IT security should collaborate in evaluating possible employee. Background checks should be done to all employees, including low-level jobs, especially in the case of technical positions, or when the applicant is technically skilled and seeking low-level position. In the interview process, there should be a technically competent person to accompany the interviewer. However, background checks are generally only cursory criminal history checks. Companies should also consider evaluating candidate's financial background. By assessing carefully candidates' criminal and financial background, the company can reduce the risk of untrustworthy employees. These employees are the ones that turn more easily into malicious insiders that seek to take advantage of the company's assets. People who have done malicious things before are more susceptible to do bad things in the future. Financial problems may indicate to gambling, drug abuse, or other social problems, and these behaviors increase the motivation to commit crimes against the employer. (Alexander, 2008 ; Cole & Ring, 2005)

As stated earlier in the chapter 3.3, disgruntled employees are the ones who might turn malicious during a convenient opportunity, and they can steal trade secrets as a vengeance towards the employer. Therefore it is crucial to take care of the employees' satisfaction in the workplace, as well as workplace retention. Employee retention requires holding onto staff by creating certain circumstances. The employer should make the employees feel welcome from the beginning with a formalized on-boarding process, as well as communicate with the employee, with one-on-one meetings if necessary. Manager's ability to recognize the employee's work and results is the most efficient way to reduce the risk of disgruntled employee. (Alexander,

2008) Employee retention is a cheaper process than continuous recruiting, and low employee turnover result in fewer recruitments, thus reducing the risk of malicious insiders.

Organizations can also control the employees' behavior with negative obligations, such as confidentiality and non-compete clauses, as well as prohibiting the exploitation of information in licensing and franchising agreements. Negative obligations consider prohibiting actions, whereas positive obligations are obliging someone to do something. Some laws specify mandatory negative obligations; however, companies should particularize the contract clauses with employees and on-site contractors, regarding to the situation and the employee's status. For instance, according to the Finnish Advocates Act (496/1958), " an advocate or his assistant shall not, without due permission, disclose the secrets of an individual or family or business or professional secrets which have come to his knowledge in the course of his professional activity." According to Norros (2012), these general provisions are not sufficient, since in the case of breach of negative obligation, the breached party usually has difficulties to evidence the suffered damages. Therefore, it is important to agree on a special contractual penalty fee. A penalty fee also helps organizations to quantify the contractual risk.

4.5 Penetration Testing

Penetration testing, especially social engineering auditing, is an effective human risk management measure to enhance the awareness of the risks. Social engineering auditing is a sort of stress testing where employees' vulnerabilities are being tested. Audits are about the company's ability to train and educate the staff, and the goals of the audits should not be to humiliate employees. Audits should be as realistic as possible in imitating real social engineering attacks, although some scope limitations apply. Depending on the country, impersonating law enforcement can be illegal; therefore, pretexting law enforcement authorities cannot be used in penetration testing activities. (Hadnagy, 2010) However, actual social engineers often masquerade themselves as law enforcement authorities to intimidate targets.

The author of the book Social Engineering – The Art of Human Hacking (2010), Christopher Hadnagy has done various social engineering audits to organizations around the world. In his book (2010), he outlines five different categories of vulnerabilities, which he afterwards evaluates for the client organization. The most important goals of audits are:

- *To determine whether employees will click on links in emails or open files from people they do not know well, leading to compromise*
- *To determine whether an employee would go to a website and enter personal or business-related information on that site*
- *To determine how much information can be obtained via the phone or in-person visits of employees at work or personal places (that is, bars, gyms, daycares)*
- *To determine the level of security in the office perimeter by testing locks, cameras, motion sensors, and security guards*
- *To determine the ability of a social engineer to create a malicious USB or DVD that will entice the employee to use it on his or her work computer, compromising the business*

(Hadnagy, 2010)

Another practical vulnerability training and testing method is called inoculation. The method is preparing the organization against a threat in a same way that inoculations boost the immune system against a disease. Organization's employees are exposed or predisposed to weakened arguments that the malicious attackers are using during the social engineering attack. The goal is to build up resistance by anticipating the malicious attackers arguments, and to prove wrong employees' false opinions about the attacks. Trainers do not have to go through long training sessions, as in awareness training. (Gragg, 2003, 12-13)

5 CONCLUSIONS

The goal of this thesis was to introduce human risk management solutions against corporate espionage by harvesting literature and prior research from various fields, such as information security, and information risk management. Organizations today have a significant amount of valuable intangible property, which can be considered trade secrets. Other corporations, states, and individuals are interested in those assets, since trade secrets can be easily monetized. Stealing valuable information assets is an ascending crime, and a huge threat to companies of any size, all around the world. These risks emanate from either outside or inside the organization.

The risk of corporate espionage is only remotely studied subject, and risk management literature provides insufficient remedies for the threat. However, the threats can cause grave troubles or even catastrophes to unprepared companies. Managing the corporate espionage should be addressed more in the risk management literature, since large part of organization's value lies in the proprietary information. Stolen or leaked blueprints of unrevealed products can destroy the whole company, because of the sunken costs in research & development, and the shortfall in revenues.

Business world today is highly dependent on information systems. Large amount of processes are automated, and their vulnerabilities are thought to be technical by nature. In addition, more and more business activities are connected to the Internet, and that is exposing information assets to new kind of risk environment – the cyber world. Information risks consist of confidentiality, integrity, and availability of information. Organizations try to protect their information assets from diverse threats, such as hackers and system errors. In order to defeat information risks, IT department must design technical security controls, such as firewalls and intrusion detection systems. However, these technical security controls are not sufficient, since human element of information risk is vital regarding to the survivability of the company. Human element is usually overlooked component of information security, and information risk management as well. As a consequence, the goal of the study was to find suitable and non-technical risk management solutions, which could help organizations to protect their valuable information assets. The second chapter introduced three integral themes relating to this

thesis, which were cyber environment, information risk, and corporate espionage. To better understand the insider and outsider threats, organizations should understand the connection between the corporate espionage attacks and information risks. Trade secret thefts are targeting information by definition, and that particular information lies under the auspices of cyber environment. These three concepts form a vantage point, through which organizations should evaluate the insider and outsider threats, and plan the risk management solutions.

Information risks and corporate espionage risks have many similarities and their interconnectivity is evident. Undoubtedly, information risk is a broader concept, since it considers all the organization's data and operational systems, and the confidentiality, integrity, and availability of information. Corporate espionage associates mostly with the confidentiality of the information. Many information risk attributes, such as cloud computing, have facilitated the execution of trade secret thefts. Internet has completely altered the risk environment of global companies. Malicious competitors and other spying actors are capable of delivering espionage attacks with smaller resources, and from far away from the target. The peculiar laws of cyber world enable continuous attacks, and foreign perpetrators are enjoying almost complete impunity, since the arm of the international law is powerless in most Internet crimes. Therefore, managing the behavior of organization's employees is an optimal approach to asserting the safety of information confidentiality. The aim of this study was not to belittle or sell short any technical security controls, since their necessity to organization's security is evident. However, the battle against corporate spies is undefeatable with mere technical solutions.

Threats to information assets are diverse, since attacks can derive from various sources. The motivation of an attack usually determines the attack vector. This thesis was about corporate espionage and trade secret threats, and the motivation behind these attacks is to gain access to other organization's trade secrets or other valuable assets. The third chapter of the thesis described two essential corporate espionage threats, which were insider threat and targeted Advanced Persistent Threat (APT). The aforementioned two attack methods are subtle and dangerous, and organizations have difficulties in evaluating, assessing, and alleviating the risks involved. APT attacks cannot be effectively prevented with technical measures, or by any measure whatsoever. Targeted attackers are persistent, and they will generally continue doing the malicious attacks until they penetrate the organization's defense. As described in chapter 3.1, attackers will plan the attacks carefully, and they go to great lengths in defeating the target organization's defense. APT attacks are also well funded, and the sophistication levels of

the organizing and planning the attacks indicate precise targeting. Targeted attacks deploy sophisticated malware as well, although the most relevant quality is the human elements of the attack; social engineering and information gathering.

The most relevant subject in this thesis was the manifold elements of malicious social engineering. Malicious cyber attackers, who are trying to steal trade secrets, use large amount of social engineering during the attacking phase. As described in chapter 3.2, employees are susceptible to be manipulated, whereas computers work in the way they are programmed. Corporate spies are using the path of least resistance when they attack an organization. In some cases, technical security controls might be difficult, if not impossible, to circumvent. Therefore, attackers are targeting humans, who are the endpoint of the computer systems. Employees make mistakes, especially when they are constantly under pressure. Malicious attackers have an arsenal of tricks how they can overload the employees' cognitive capabilities, and make the targeted employees to divulge information. By far, the most common attack method is the traditional phone, and email is a popular method as well. However, phone calls give the targets less time to think the caller's request. Malicious attackers use human related vulnerabilities in accordance with manipulative tricks to build trust between the caller and the target. Social engineers are well prepared for the attack, since they do a large amount of information gathering prior the attack. Social engineers have a believable pretext that they use in order to elicit valuable information. Corporate spies can either elicit trade secrets directly or gather login and user credentials for later use. Either way, social engineering is an extremely complex but efficient tool for targeted threats. Altogether, the social engineering chapter shed light on the difficult and mischievous threat to organization's data assets. The goal of analyzing social engineering was to introduce the manifold attack methods, and to delineate the magnitude of the risk for the organization's competitive contingency.

Social engineering is not the only attack method of corporate spies. Another stealthy way of spying companies is to use insiders. There are many types of insiders, with various motivations and goals, and this fact makes it extremely hard for an organization to observe malicious or threatening activity. Organizations must find a balance between healthy skepticism and paranoia. Companies should not start persecuting or victimizing employees without airtight evidence. Nevertheless, any suspicious activity should be taken seriously. As described in chapter 3.3, diminished loyalty towards an employer has caused dissatisfaction at workplaces. Employers should observe at least two aspects regarding to insider threats. First thing is the

motivation to commit trade secret thefts, since employees have various problems that lead to desperate solutions. Secondly, employers should control the situations, where employees have convenient opportunity to steal valuable data assets. The assessment of the insider risk is important for managers, since they must recognize the threat, and the consequences of the realized risk. The main point of the insider threat chapter was to familiarize the risk, and make a comparison with social engineering. Malicious insider activities are more commonplace problems of large economic superpowers, such as in the U.S. and Germany. However, insider attacks occur in Finland as well (see chapter 3.3.5). An efficient natural obstacle for social engineers in Finland is the complex language, which complicates the attacking methods. However, many multinational companies in Finland use English as official working language; hence, social engineers can approach the targets without translators.

The second chapter in this thesis introduced the risk environment, and chapter number three outlined two corporate espionage threats. The goal of the third chapter was to assess the risks of social engineering and insider threats. However, these assessed corporate espionage risks needed mitigation controls as well. The aim of the fourth chapter was to introduce the most effective risk controls and solutions to mitigate corporate espionage risks. The scope of this thesis was on the human risk management controls; therefore, all the technical and physical solutions were left out from the scope of this study. As stated earlier in chapter 2.3, in the case of corporate espionage, companies usually do not have any recourse to the law. Therefore, companies must seek other remedies to battle against the insider and outsider threats.

As introduced in the second chapter, one of the biggest impediments of information security is that a separate technical department is controlling the information risks. Organizations should facilitate the communication between IT personnel and other managers, and all decisions should align with the organization's overall risk management strategy. Enterprise Risk Management (ERM) is an optimal tool for this. The goal of the ERM is to align all departments together, in order to provide harmonized risk analysis for the board. IT security has its own peculiarities, since it contains technical jargon that is incomprehensible to other managers. In order to mitigate corporate espionage, some important issues should be considered in the operational and strategic risk management procedures. These important issues are data classification, awareness of the threats, policies and guidelines, and penetration testing. With a profound research of literature, these areas were the most convenient and effective risk management controls against social engineering and insider threats.

In the beginning of the research, prior exploring the literature, I was not aware how important part the data classification procedures would be in this thesis. However, organizations have to acknowledge the importance of efficient and secure data management. All employees should know the reasons why each classified data asset is protected. Mere authentication policies are not sufficient, if employees do not fathom the reasoning behind it. Employees make security tradeoffs if the security measures cause inconvenience. The situation could be different if employees knew the rationale behind the compulsory security measures. Each valuable information asset that is susceptible to corporate espionage should have an owner, custodian, and user. This classification technique clarifies the reporting and documenting roles of each classified data.

Threat awareness is a closely related subject to data classification. By raising awareness, it is possible to steer the employees' behavior. Data classification considers why valuable data is in need of protection, while threat awareness is about recognizing the attacks and knowing the motivations behind the attacks. It is safe to say, that many organizations rely on the assumption that "corporate espionage could not happen to us". Extreme risks are likely to cause "us and them" –thinking, where people identify one's own organization as safer than other organizations. Therefore, the starting phase of the corporate espionage risk management process is to accept the existence of social engineering and insider threats. The awareness of the risk was essential point of this research, since it aligns with all the other risk controls, which are data classification, policies and guidelines, and penetration testing.

The third chapter outlined the peculiarities and effectiveness of targeted threats, and the chapter 4.3 outlined the importance of recognizing those threats. Social engineering is a collection of deceptive tools, and organization's employees have to be aware of those tricks, and how attackers can approach target employees with malicious incentives. En example of effective risk management solution is to go through social engineering cases. This is a practical way to enhance the awareness of the risk. From the case based learning, employees could observe how social engineers can elicit pieces of mundane information, and how the attackers are using the mundane information to approach other employees. Even though social engineering attacks are unique, they have many similarities, and their socio-psychological effect relies on the few attributes that were introduced in the chapter 3.2. Employees should be taught to respond correctly to weird requests, and through awareness training, organizations should

demonstrate the manifold ways social engineers might approach the organization's employees. Awareness training should be systematic and dynamic. Each employee should participate in the training, and the trainings should be repeated at certain intervals.

The most concrete way to direct the behavior of organization's employees is to add strict and precise policies, which will guide the employee's actions in abnormal situations. Policy implementing and awareness training should go hand in hand, since they are pretty much useless without the other. Policies have no function if employees do not obey them or understand them. Vice versa, awareness training is a waste of time if organization is not guiding the behavior with strict rules. Neglecting the policies will lead to an organizational culture of neglect. Therefore, policy development should be a well-planned process, where various departments should collaborate. One big mistake is to assess the policies in total isolation from risk management strategy and data classification processes. It is also crucial to remember that organizational habits can sometimes be deeply embedded in the organizational culture, and they are not easily changed. Policies and guidelines should be evaluated continuously, since the attack methods and attack vectors are changing all the time. This is due to the inconsistent nature of information risk environment, where short technical development circles change the risks constantly.

However, steering the behavior of employees with policies is not a panacea in thwarting trade secret thefts. Sometimes, there are no such policies or behavioral codes of conduct that would reduce the risk of successful elicitation. Especially when the social engineers are extremely skillful professionals. Respectively, some malicious insiders are extremely carefully hiding their trade secret thefts, and the organization has no remedies for the problem.

The final risk management solution is to test the organization's human vulnerabilities. Vulnerability is a flaw or weakness in the asset's defense, and the objective of penetration testing is to strengthen the asset's defense. Penetration testing is a critical risk management phase, since it is giving immediate feedback from the organization's defense and risk controls. It is obvious that organizations should act in accordance with the feedback. The objective is to find where in the organization the vulnerabilities exist, and afterwards adjust the vulnerabilities. With the right kind of vulnerability testing, the organization can get more resilient in the cases of real threat. In addition, penetration testing is raising awareness of the possible threats and attack methods.

Before writing this literature review, I noticed that most efforts to improve information security focused on the technological approaches. Organizations are extremely concerned about the functionality of their systems and programs; therefore, it is obvious that the cyber security thinking is largely technical. However, human element is important in the cyber security, and in order to build more efficient defense, organizations have to start managing the human behavior more consistently. The research literature revealed large amount of human related measures to improve cyber security. These non-technical solutions towards cyber security were mostly related to data management and policies. The other vantage point of this research was corporate espionage, which is reasonably old threat for organizations. Corporate espionage provided a scope and a direction for this literature review. In the risk management literature, the risk of trade secret thefts is a small-scale topic. Malicious insider activity and social engineering are both severe risks to organizations. The risk of abusive trust should be more known to risk managers.

Since the corporate espionage activity has spread to all corners of the world, all risk management controls introduced in this thesis applies to Finnish organizations as well. Companies that generate innovations should carefully assess insider and outsider threats. Even start-up companies or one-man companies should not completely ignore the dangers of corporate espionage.

Insider threats and social engineering are both interesting research topics, and an example of future research would be the problems with insider activity and employees' privacy matters. An excessive paternalism is a poor alternative, but employees should be constantly under some sort of supervision and control. Another extremely interesting research topic would be to evaluate the correlation between security policies and organizational habits. Old habits die hard; hence, it would be interesting to study the changes in the employees' behavior on the verge of policy change.

References

Literature Sources:

Aaron, Greg .2014. Phishing Activity Trends Report APWG

Alexander, Philip. 2008. Information Security: A Manager's Guide to Thwarting Data Thieves and Hackers.

Ask, Merete, et al. 2013. Advanced Persistent Threat (APT) Beyond the hype.

Bandyopadhyay, T., Mookerjee, V. S., & Rao, R. C. 2009. Why IT managers don't go for cyber-insurance products. Communications of the ACM, 52(11), 68-73.

Baumeister, Roy F. & Leary, Mark, R. 1997. Writing narrative literature reviews. Review of general psychology 1.3: 311.

Biener, Christian, Eling, Martin, & Wirfs, Jan H. 2015. Insurability of Cyber Risk: An Empirical Analysis. The Geneva Papers on Risk and Insurance-Issues and Practice 40.1: 131-158.

Bodeau, Deborah & Graubart, Richard. 2011. Cyber Resiliency Engineering Framework.

Bojanc, Rok, and Borka Jerman-Blažič. 2008. An economic modelling approach to information security risk management. International Journal of Information Management 28.5: 413-422.

Botelho, Christopher M. & Cazier, Joseph A. 2008. Guarding Corporate Data from Social Engineering Attacks. Handbook of Research on Information Security and Assurance.

Brewer, Ross. Advanced persistent threats: minimising the damage. Network Security 2014.4 (2014): 5-9.

Burgess, Christopher & Power, Richard. Secrets stolen, fortunes lost: Preventing intellectual property theft and economic espionage in the 21st century. Syngress, 2011.

Chernobai, Anna, Rachev, Svetlozar T. & Fabozzi Frank. 2008. Operational risk: a guide to Basel II capital requirements, models, and analysis. Vol. 180. John Wiley & Sons.

Choo, Kim-Kwang Raymond. 2011. The cyber threat landscape: Challenges and future research directions. Computers & Security 30.8 : 719-731.

Cole, Eric. 2002. Hackers beware. Sams Publishing.

Cole, Eric. 2012. Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization. Newnes.

Cole, Eric & Ring, Sandra. 2005. Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft: Protecting the Enterprise from Sabotage, Spying, and Theft. Syngress.

Coskun Samli, A. & Jacobs, Laurence. 2003. Counteracting global industrial espionage: a damage control strategy." Business and Society Review 108.1: 95-113.

Dontamsetti, Mahi & Narayanan, Anup. 2008. Impact of the Human Element on Information Security. In Gupta, Manish, ed. Social and Human Elements of Information Security: Emerging Trends and Countermeasures: Emerging Trends and Countermeasures. IGI Global.

Duhigg, Charles. 2012. The power of habit: Why we do what we do in life and business. Random House.

Fink, Steven. 2002. Sticky fingers: Managing the global risk of economic espionage. Dearborn Trade Pub.

Finney, Nathan K. 2014. Cybersecurity and Cyberwar: What Everyone Needs to Know. Parameters 44.3.

Ghormley, Yvette. 2008. Security Policies and Procedures Gupta, Jatinder ND, ed. Handbook of research on information security and assurance. IGI Global, 2008

Giura, Paul, & Wang, Wie. 2013. Using large scale distributed computing to unveil advanced persistent threats. SCIENCE 1.3.

Gragg, David. 2003. A multi-level defense against social engineering. SANS Reading Room, March 13.

Granger, Sarah. 2001. Social engineering fundamentals, part I: hacker tactics. Security Focus, December 18.

Gregory, Peter. 2003. Enterprise Information Security, Financial Times Management.

Gupta, Jatinder N.D. & Sharma, Sushil K. In Gupta, Jatinder ND, ed. Handbook of research on information security and assurance. IGI Global, 2008.

Hadnagy, Christopher. 2010. Social engineering: The art of human hacking. John Wiley & Sons.

Hamdi, M., Doudriga, N., & Obaidat, M. 2006. Security Policy Guidelines. H. Bidgoli, Handbook of Information Security, Information Warfare, Social, Legal, and International Issues and Security Foundations (Vol. 2). John Wiley & Sons.

Hampton, John J. 2009. Fundamentals of enterprise risk management: How top companies assess risk, manage exposure, and seize opportunity. AMACOM Div American Mgmt Assn.

Heikkinen, Seppo. 2006. Social engineering in the world of emerging communication technologies. the Proceedings of Wireless World Research Forum meeting. Vol. 17.

Hoanca, Bogdan, & Mock, Kenrick. 2008. Effects of Digital Convergence on Social Engineering Attack Channels. Social and Human Elements of Information Security: Emerging Trends and Countermeasures: Emerging Trends and Countermeasures.

Jerman-Blažič, Borka. 2008. An economic modelling approach to information security risk management. International Journal of Information Management 28.5.

Kaspersky Lab ZAO 2013. Global Corporate IT Security Risk: 2013.

Kramer, L. A., Heuer Jr, R. J., & Crawford, K. S. 2005. Technological, social, and economic trends that are increasing US vulnerability to insider espionage. DEFENSE PERSONNEL SECURITY RESEARCH CENTER MONTEREY CA.

Laaksonen, Mika, Nevasalo, Terho, & Tomula, Karri. 2006. Yrityksen tietoturvakäsikirja: ohjeistus, toteutus ja lainsäädäntö. Edita.

Lam, James. 2014. Enterprise risk management: from incentives to controls. John Wiley & Sons.

Limnéll Jarmo, Majewski Klaus, Salminen Mirva. 2014. Kyberturvallisuus, Jyväskylä.

Long, Johnny. 2011. No tech hacking: A guide to social engineering, dumpster diving, and shoulder surfing. Syngress.

Maynard, S., & Ruighaver, A. B. 2006. What makes a good information security policy: A preliminary framework for evaluating security policy quality.

McBride, George. 2003. In Tipton, Harold F., and Micki Krause. Information security management handbook. CRC Press.

Mitnick, Kevin D. & Simon, William, L. 2011. The art of deception: Controlling the human element of security. John Wiley & Sons.

Molok, Nurul, Abdul, Nuha, Chang, Shanton & Ahmad, Atif. 2010. Information leakage through online social networking: Opening the doorway for advanced persistence threats.

Moore, Tyler, Pym, David J. & Ioannidis, Christos. 2010. Economics of information security and privacy. Springer.

Nasheri, Hedieh. 2005 Economic espionage and industrial spying. Cambridge University Press.

Nayak, Umesha & Rao, Umesh, Hodeghatta. 2014. The InfoSec Handbook: An Introduction to Information Security. Apress.

Nohlberg, Marcus. 2008. Why Humans are the weakest Link. Gupta, M. and Sharman, R. Social and Human Elements in Information Security: Emerging Trends and Countermeasures, IGI Global, Hershey, USA.

Norros, Olli. 2012. Velvoiteoikeus. Sanoma Pro Oy, Helsinki.

O`Hara, Gerard. 2010. Cyber-Espionage: A Growing Threat to the American Economy. CommLaw Conspectus, 19, 241.

Peltier, Thomas R. 2001. Information Security Policies, Procedures, and Standards: guidelines for effective information security management. CRC Press.

Peltier, Thomas R. 2005. Implementing an Information Security Awareness Program. Information Systems Security.

Peltier, Thomas R. 2013. Information security fundamentals. CRC Press.

Ponemon Institute. 2012. The Impact of Cybercrime on Business

Rees, Jackie, Bandyopadhyay, Subhajyoti & Spafford, Eugene H. 2003. PFIRES: a policy framework for information security. Communications of the ACM.

Reisman, Arnold. 2006. A taxonomic view of illegal transfer of technologies: A case study. Journal of Engineering and Technology Management.

Rogers, Marcus K. 2007. Social Engireering: The Human Factor of Information Assurance. In Tipton, Harold, F. & Micki Krause. Information security management handbook. CRC Press.

Rudolph, K. 2006. Implementing a Security Awareness Program. Handbook of Information Security.

Salminen, Ari. 2011. Mikä kirjallisuuskatsaus. Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin. Vaasan yliopiston julkaisuja. Opetusjulkaisuja 62.

Sandelowski, Margarete. 1991. Telling stories: Narrative approaches in qualitative research. Image: the journal of nursing scholarship 23.3.

Shaurette, Ken M. & Schleppenbach, Tom. 2013. In O'Hanley, Richard & Tiller, James, S. eds. Information Security Management Handbook. Vol. 7. CRC Press.

Skinner, Christina Parajon. 2013. International Law Response to Economic Cyber Espionage, An. Conn. L. Rev. 46.

Simon, Spencer. 1998. Economic Espionage Act of 1996, The. Berkeley Tech. LJ13.

Symantec. 2011. CUTTING THROUGH THE HYPE Advanced Persistent Threats: A Symantec Perspective. Preparing the Right Defense for the New Threat Landscape. White Paper.

Tankard, Colin. 2011. Advanced Persistent threats and how to monitor and deter them. Network security 2011.8.

Tankard, Colin. 2014. New rules for combating new threats. Computer Fraud & Security 2014.4

Thonnard, Olivier, et al. 2012. Industrial espionage and targeted attacks: Understanding the characteristics of an escalating threat. Research in attacks, intrusions, and defenses. Springer Berlin Heidelberg.

Torres, Jose M., Sarriegi, Jose, M. & Santos Javier. 2008. Critical Success Factors and Indicators to Improve Information Systems Security Management Actions. In Handbook of Research on Information Security and Assurance 160000.

Winkler, Ira S. 1996. Case study of industrial espionage through social engineering. Proceedings of 19th national information systems security conference.

Internet Sources:

ACAD/Medre.A Worm Uncovered: Steals AutoCAD Design Files From Peru and Other Countries, Sends Them To China. [accessed on 15/3/2015]
mytechguide.org/12485/acad-medrea-worm-uncovered-steals-autocad-design-files/

Act on the Protection of Privacy in Electronic Communications. 516/2004.
finlex.fi

Advocates Act. 496/1958. Ministry of Justice, Finland.
finlex.fi/en/laki/kaannokset/1958/en19580496

Chronology of Data Breaches. [accessed on 1/2/2015]
privacyrights.org/data-breach

Criminal Code. 39/1889. Ministry of Justice, Finland.
finlex.fi/en/laki/kaannokset/1889/en18890039

Europe's Weaker Laws Against Trade Secret Theft Means Corporate Espionage Often Goes Unpunished. August 5, 2011.
businessinsider.com/europes-lack-of-trade-secret-theft-protection-laws-means-coprorate-espionage-often-goes-unpunished-2011-8?IR=T

How to Thwart a Social Engineering Exploit. 2015. [accessed on 10/2/2015]
www.t2pa.com/project-reality-based-guides

Information Society Code. 917/2014. Ministry of Transportation and Communication, Finland.
http://finlex.fi/en/laki/kaannokset/2014/en20140917

KKO:2013:20 Case from the Supreme Court of Finland. April 5, 2013.
finlex.fi/fi/oikeus/kko/kko/2013/20130020

NIST SP 800-39 Appendix B. [accessed on 22/3/2015]
fismapedia.org/index.php/NIST_SP_800-39_Appendix_B

searchsecurity.techtarget.com/definition/attack-vector [accessed on 22/3/2015]